S5850 and S8050 Series Switches CLI Reference Guide

Models: S5850-32S2Q; S5850-48S6Q; S5850-48S2Q4C; S5850-48T4Q; S8050-20Q4C
# Contents

Chapter 1 Preface.................................................................................................................................................. 1
  1.1 Declaration.................................................................................................................................................. 1
  1.2 Audience.................................................................................................................................................... 1
  1.3 Conventions.............................................................................................................................................. 1

Chapter 2 Basic Commands................................................................................................................................. 2
  2.1 System Configuration Commands........................................................................................................... 2
  2.2 User Management Commands.................................................................................................................. 60
  2.3 FTP Commands.......................................................................................................................................... 66
  2.4 TFTP Commands....................................................................................................................................... 74
  2.5 scp Commands........................................................................................................................................... 78
  2.6 Telnet Commands...................................................................................................................................... 81
  2.7 SSH Commands......................................................................................................................................... 85
  2.8 Time&Timezone Commands....................................................................................................................... 107
  2.9 License Commands.................................................................................................................................... 112
  2.10 HTTP commands Commands................................................................................................................ 114
  2.11 RPC-API commands Commands........................................................................................................... 123

Chapter 3 Ethernet Commands............................................................................................................................ 126
  3.1 Interface Commands................................................................................................................................ 126
  3.2 Interface Errdisable Commands............................................................................................................... 147
  3.3 MAC Address Table Commands............................................................................................................... 154
  3.4 VLAN Commands.................................................................................................................................... 164
  3.5 Voice VLAN Commands............................................................................................................................ 178
  3.6 Link Aggregation Commands.................................................................................................................... 181
  3.7 VLAN Classification Commands............................................................................................................. 198
  3.8 VLAN Mapping Commands....................................................................................................................... 203
  3.9 MSTP Commands..................................................................................................................................... 215
  3.10 Flow Control Commands......................................................................................................................... 245
  3.11 Priority-based Flow Control Commands............................................................................................... 247
  3.12 Layer 2 Protocols Tunneling Commands............................................................................................... 249
  3.13 Storm Control Commands...................................................................................................................... 255
  3.14 Loopback Detection Commands............................................................................................................ 257
  3.15 MLAG Commands.................................................................................................................................. 262

Chapter 4 IP Service Commands......................................................................................................................... 270
  4.1 ARP Commands....................................................................................................................................... 270
  4.2 DHCP Client Commands........................................................................................................................... 286
  4.3 DHCP Relay Commands............................................................................................................................ 300
  4.4 DHCP Server Commands.......................................................................................................................... 316

www.fs.com
14.3 Mirror Commands.................................................................................................................. 1362
14.4 Device Management Commands.......................................................................................... 1374
14.5 Bootrom Commands............................................................................................................ 1379
14.6 Bootup Diagnostic Commands.............................................................................................. 1386
14.7 SmartConfig Commands..................................................................................................... 1387
14.8 Debian Commands.............................................................................................................. 1389

Chapter 15 Network Management Commands.......................................................................... 1390
15.1 Network Diagnosis Commands.......................................................................................... 1390
15.2 NTP Commands................................................................................................................ 1392
15.3 Phy Loopback Commands.................................................................................................. 1405
15.4 RMON Commands........................................................................................................... 1412
15.5 SNMP Commands.............................................................................................................. 1419
15.6 SFlow Commands............................................................................................................. 1439
15.7 LLDP Commands.............................................................................................................. 1444
15.8 IPFIX Commands.............................................................................................................. 1457

Chapter 16 VPN Commands...................................................................................................... 1485
16.1 VRF Commands................................................................................................................ 1485
16.2 GRE TUNNEL Commands.................................................................................................. 1498
16.3 ERSPAN TUNNEL Commands.......................................................................................... 1508

Chapter 17 Data Center Commands.......................................................................................... 1517
17.1 Overlay Commands............................................................................................................. 1517
17.2 PFC Commands................................................................................................................ 1532
17.3 EFD Commands................................................................................................................. 1535
17.4 Flow hash Commands....................................................................................................... 1549
17.5 OVSDB Commands........................................................................................................... 1550
17.6 EVPN Commands.............................................................................................................. 1555

Chapter 18 MPLS Commands..................................................................................................... 1585
18.1 LDP Commands................................................................................................................ 1585
18.2 MPLS Commands.............................................................................................................. 1623
18.3 VPLS Commands.............................................................................................................. 1633
18.4 VPWS Commands............................................................................................................. 1646
Chapter 1 Preface

1.1 Declaration

This document updates at irregular intervals because of product upgrade or other reason. This document is for your reference only.

1.2 Audience

This document is for the following audiences:

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

1.3 Conventions

Command syntax convention table

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Italic type with capital letters</strong></td>
<td>Use italic type with capital letters for the parameters of the commands. Parameters are the parts which need to replace with the actual value.</td>
</tr>
<tr>
<td>(x</td>
<td>y</td>
</tr>
<tr>
<td>(x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>&lt;x-y&gt;</td>
<td>Select a number between x and y.</td>
</tr>
</tbody>
</table>
Chapter 2 Basic Commands

2.1 System Configuration Commands

2.1.1 hostname

Command Purpose

To specify or modify the host name for the network server, use the “hostname” command in Global Configuration. To restore the configuration to the default, use the “no hostname” command.

Command Syntax

hostname NAME
no hostname

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>New host name for the network server</td>
<td>Host name is a string with 1-63 characters</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D/M</td>
<td>The management IPv4 address with mask length configured</td>
<td>IPv4 address with mask length 1-32</td>
</tr>
<tr>
<td>A.B.C.D mask</td>
<td>The management IPv4 address and mask configured</td>
<td>IPv4 address and mask</td>
</tr>
<tr>
<td>X:X::X:X/M</td>
<td>The management IPv6 address with mask length configured</td>
<td>IPv6 address with mask length 1-128</td>
</tr>
<tr>
<td>X:X::X:X mask</td>
<td>The management IPv6 address and mask configured</td>
<td>IPv6 address and mask</td>
</tr>
<tr>
<td>gateway A.B.C.D</td>
<td>Add IPv4 gateway</td>
<td>IPv4 address</td>
</tr>
<tr>
<td>gateway X:X::X:X</td>
<td>Add IPv6 gateway</td>
<td>IPv6 address</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Add the route</td>
<td>-</td>
</tr>
<tr>
<td>del</td>
<td>Del the route</td>
<td>-</td>
</tr>
<tr>
<td>ipv6</td>
<td>Configure IPv6 gateway</td>
<td>-</td>
</tr>
<tr>
<td>gateway</td>
<td>Add gateway</td>
<td>-</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>The IPv4 address of the gateway</td>
<td>IPv4 address</td>
</tr>
<tr>
<td>X:X::X:X</td>
<td>The IPv6 address of the gateway</td>
<td>IPv6 address</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Address</th>
<th>Hardware Addr</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.39.254</td>
<td>00:1e:08:09:67:6d</td>
<td>mgmt-if</td>
</tr>
</tbody>
</table>
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::1/96
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
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`
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege LEVEL</td>
<td>User privilege level</td>
<td>Level value &lt;1-4&gt;</td>
</tr>
<tr>
<td>8</td>
<td>Specifies a hidden password will follow</td>
<td>-</td>
</tr>
<tr>
<td>LINE</td>
<td>The password string</td>
<td>-</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LENGTH</td>
<td>Number of lines on the screen</td>
<td>The value is a number from 0 to 512. A value of zero disables pausing between screens of output</td>
</tr>
</tbody>
</table>

**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 Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LENGTH</td>
<td>Number of lines on the screen</td>
<td>The value is a number from 0 to 512. A value of zero disables pausing between screens of output</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

None

**Usage**

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

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

**Examples**

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

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

**Related Commands**

terminal length

---

### 2.1.11 banner motd

**Command Purpose**

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

**Command Syntax**

```
banner motd line
no banner motd
```
Parameter | Parameter Description | Parameter Value
--- | --- | ---
LINE | message string | specify a visible character as delimiting character, enter the message between 2 delimiting characters. At most support 99 lines with 1023 character in each line

**Command Mode**

Global Configuration

**Default**

None

**Usage**

None

**Examples**

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

Switch# configure terminal
Switch(config)# banner motd #

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

**Related Commands**

banner exec
banner login

**2.1.12 banner exec**

**Command Purpose**

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

**Command Syntax**

banner exec line
no banner exec
### 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 Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LINE</td>
<td>message string</td>
<td>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</td>
</tr>
</tbody>
</table>

#### Command Mode

Global Configuration

**Default**

None

**Usage**

None

**Examples**

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

```plaintext
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**

```plaintext
show version { slot ID | } 
```


<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>slot id</td>
<td>1-29</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAX_VTY</td>
<td>Max login VTY</td>
<td>The default value is 8. range &lt;0-8&gt;</td>
</tr>
<tr>
<td>VTY</td>
<td>Number of VTY</td>
<td>Range &lt;0-7&gt;</td>
</tr>
</tbody>
</table>

**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 does 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MINUTES</td>
<td>Timeout in minute</td>
<td>Range &lt;0-35791&gt;</td>
</tr>
<tr>
<td>SECONDS</td>
<td>Timeout in second</td>
<td>Range &lt;0-2147483&gt;</td>
</tr>
</tbody>
</table>

Command Mode

Line Configuration

Default

600 seconds

Usage

When the user login again then config will be effective.

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
Switch(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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL-NAME</td>
<td>The name of the IPv4 acl</td>
<td>A string with up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode
Line Configuration

Default
No ACL

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

Examples
The following example shows how to apply IPv4 ACL on vty:
Switch(config-line)# access-class acl4 in

Related Commands

ip access-list

2.1.18 ipv6 access-class

Command Syntax

ipv6 access-class ACL-NAME in
no ipv6 access-class in

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL-NAME</td>
<td>The name of the IPv6 acl</td>
<td>A string with up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode
Line Configuration
Default

No ACL

Usage

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

Examples

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

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

Related Commands

ipv6 access-list

2.1.19 reboot

Command Purpose

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

Command Syntax

reboot

Command Mode

Privileged EXEC

Default

None

Usage

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

Examples

The following example is sample dialog from the reboot command:
Switch# reboot

Related Commands

reload

2.1.20 schedule reboot at

Command Purpose

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

Command Syntax

schedule reboot at HH:MM (MM/DD | MM/DD/YYYY | YYYY/MM/DD)
no schedule reboot

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

Command Mode

Global Configuration

Default

No scheduled reboot task is defined.

Usage

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

Examples

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

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

schedule reboot delay

2.1.21 schedule reboot delay

Command Purpose

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

Command Syntax

schedule reboot delay {HH:MM | MINUTES}
no schedule reboot

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HH:MM</td>
<td>The hour and minutes</td>
<td>The time range is 00:00 – 23:59</td>
</tr>
<tr>
<td>MINUTES</td>
<td>The minutes</td>
<td>The range is 1-720</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

No scheduled reboot task is defined.

Usage

None

Examples

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

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

Related Commands

schedule reboot at
2.1.22 boot system

Command Purpose

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

Command Syntax

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

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

Command Mode

Privileged EXEC

Default

None

Usage

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

Examples

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

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

Related Commands

show boot

2.1.23 show boot

Command Purpose

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

show boot

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show boot command:

```
Switch# show boot
The current boot image version is: E330-3.0.0.23.it
The current running image is: tftp://10.10.29.160/humberOS-e330-ma-v3.0.0.23.it.r.bin
The next running image is: tftp://10.10.29.160/humberOS-e330-ma-v3.0.0.23.it.r.bin
```

Related Commands

show boot images

2.1.24 show boot images

Command Purpose

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

Command Syntax

show boot images

Command Mode

Privileged EXEC
Default

None

Usage

None

Examples

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

```
Switch# show boot images
System image files list:
Current boot image version: 1.0.0.25

<table>
<thead>
<tr>
<th>Create Time</th>
<th>Version</th>
<th>File name</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 2011-07-25 10:58:29</td>
<td>v3.0.0.22lt</td>
<td>Internal-.00.22.bin</td>
</tr>
</tbody>
</table>
```

Related Commands

show boot

2.1.25 show memory

Command Purpose

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

Command Syntax

```
show memory ( all | bgp | bhm | chsm | dhclient | dot1x | ini | ipv6 | lacp | ldp | lib | mstp | nsm | oamd | onmd | ospf | pim | ptp | rip | rsvp | shal | summary )
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>All memory information</td>
<td>-</td>
</tr>
<tr>
<td>bgp</td>
<td>Border Gateway Protocol (BGP)</td>
<td>-</td>
</tr>
<tr>
<td>bhm</td>
<td>Health monitoring</td>
<td>-</td>
</tr>
<tr>
<td>chsm</td>
<td>Chassis management</td>
<td>-</td>
</tr>
<tr>
<td>dhclient</td>
<td>DHCP client module</td>
<td>-</td>
</tr>
<tr>
<td>dhcpd</td>
<td>DHCP</td>
<td>-</td>
</tr>
<tr>
<td>dhcprelay</td>
<td>DHCP relay</td>
<td>-</td>
</tr>
<tr>
<td>dhcprelay6</td>
<td>DHCP relay6(IPv6)</td>
<td>-</td>
</tr>
<tr>
<td>dot1x</td>
<td>IEEE 802.1X Port-Based Access Control</td>
<td>-</td>
</tr>
<tr>
<td>imi</td>
<td>Integrated Management Interface (IMI)</td>
<td>-</td>
</tr>
<tr>
<td>ipv6</td>
<td>Internet Protocol version 6 (IPv6)</td>
<td>-</td>
</tr>
<tr>
<td>lacp</td>
<td>Link Aggregation Control Protocol (LACP)</td>
<td>-</td>
</tr>
<tr>
<td>ldp</td>
<td>Label Distribution Protocol (LDP)</td>
<td>-</td>
</tr>
<tr>
<td>lib</td>
<td>Library information</td>
<td>-</td>
</tr>
<tr>
<td>mstp</td>
<td>Spanning Tree Protocols (STP/RSTP/MSTP)</td>
<td>-</td>
</tr>
<tr>
<td>nsmd</td>
<td>Network Service Module (NSM)</td>
<td>-</td>
</tr>
<tr>
<td>oam</td>
<td>Bidirectional Forwarding Detection (BFD)</td>
<td>-</td>
</tr>
<tr>
<td>onmd</td>
<td>LLDP and EFM, OAM</td>
<td>-</td>
</tr>
<tr>
<td>ospf</td>
<td>Open Shortest Path First (OSPF)</td>
<td>-</td>
</tr>
<tr>
<td>pim</td>
<td>Protocol Independent Multicast (PIM)</td>
<td>-</td>
</tr>
<tr>
<td>ptp</td>
<td>Precision Time Protocol (PTP)</td>
<td>-</td>
</tr>
<tr>
<td>rip</td>
<td>Routing Information Protocol (RIP)</td>
<td>-</td>
</tr>
<tr>
<td>rsvp</td>
<td>Resource Reservation Protocol (RSVP)</td>
<td>-</td>
</tr>
<tr>
<td>shal</td>
<td>Hal server monitoring</td>
<td>-</td>
</tr>
<tr>
<td>summary</td>
<td>Summary memory information</td>
<td>-</td>
</tr>
<tr>
<td>monitor</td>
<td>monitor</td>
<td>-</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Memory type</th>
<th>Alloc cells</th>
<th>Alloc bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temporary memory</td>
<td>6596</td>
<td>322216</td>
</tr>
<tr>
<td>Hash</td>
<td>10</td>
<td>320</td>
</tr>
<tr>
<td>Hash index</td>
<td>10</td>
<td>40960</td>
</tr>
<tr>
<td>Hash bucket</td>
<td>55</td>
<td>880</td>
</tr>
<tr>
<td>Link list</td>
<td>13</td>
<td>400</td>
</tr>
<tr>
<td>Link list node</td>
<td>115</td>
<td>1840</td>
</tr>
<tr>
<td>Show</td>
<td>1</td>
<td>512</td>
</tr>
<tr>
<td>Show page</td>
<td>1</td>
<td>8192</td>
</tr>
<tr>
<td>Show server</td>
<td>1</td>
<td>64</td>
</tr>
<tr>
<td>Prefix IPv4</td>
<td>6</td>
<td>48</td>
</tr>
<tr>
<td>Route table</td>
<td>6</td>
<td>48</td>
</tr>
<tr>
<td>Route node</td>
<td>309</td>
<td>19776</td>
</tr>
<tr>
<td>Vector</td>
<td>3383</td>
<td>324768</td>
</tr>
<tr>
<td>Vector index</td>
<td>3383</td>
<td>48824</td>
</tr>
<tr>
<td>SNMP subtree</td>
<td>8</td>
<td>6144</td>
</tr>
<tr>
<td>Host config</td>
<td>1</td>
<td>16</td>
</tr>
<tr>
<td>Message of The Day</td>
<td>1</td>
<td>128</td>
</tr>
<tr>
<td>IMI Client</td>
<td>2</td>
<td>1056</td>
</tr>
<tr>
<td>VTY master</td>
<td>1</td>
<td>16</td>
</tr>
<tr>
<td>VTY if</td>
<td>52</td>
<td>39936</td>
</tr>
<tr>
<td>VTY connected</td>
<td>3</td>
<td>192</td>
</tr>
<tr>
<td>Message handler</td>
<td>2</td>
<td>128</td>
</tr>
<tr>
<td>Host</td>
<td>1</td>
<td>96</td>
</tr>
<tr>
<td>Log information</td>
<td>2</td>
<td>128</td>
</tr>
<tr>
<td>Context</td>
<td>1</td>
<td>512</td>
</tr>
</tbody>
</table>

Memories for BGP

<table>
<thead>
<tr>
<th>Memory type</th>
<th>Alloc cells</th>
<th>Alloc bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP structure</td>
<td>1</td>
<td>768</td>
</tr>
<tr>
<td>BGP VR structure</td>
<td>1</td>
<td>384</td>
</tr>
<tr>
<td>BGP global structure</td>
<td>1</td>
<td>64</td>
</tr>
<tr>
<td>BGP peer</td>
<td>1</td>
<td>2048</td>
</tr>
<tr>
<td>Ext community</td>
<td>1</td>
<td>16</td>
</tr>
<tr>
<td>BGP as list master</td>
<td>1</td>
<td>32</td>
</tr>
<tr>
<td>Community list handler</td>
<td>1</td>
<td>32</td>
</tr>
</tbody>
</table>
```
BGP Damp Reuse List Array : 1 2048
BGP table : 31 248
BGP VRF list : 1 64

Related Commands

show processes memory sorted

2.1.26 show cpu traffic-limit

Command Purpose

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

Command Syntax

show cpu traffic-limit

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

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

Switch# show cpu traffic-limit

<table>
<thead>
<tr>
<th>reason</th>
<th>rate (pps)</th>
<th>class</th>
</tr>
</thead>
<tbody>
<tr>
<td>bpdu</td>
<td>64</td>
<td>3</td>
</tr>
<tr>
<td>cfm</td>
<td>512</td>
<td>2</td>
</tr>
<tr>
<td>slow-protocol</td>
<td>128</td>
<td>1</td>
</tr>
<tr>
<td>eapol</td>
<td>128</td>
<td>0</td>
</tr>
<tr>
<td>erps</td>
<td>128</td>
<td>2</td>
</tr>
<tr>
<td>smart-link</td>
<td>128</td>
<td>2</td>
</tr>
<tr>
<td>udld</td>
<td>128</td>
<td>3</td>
</tr>
<tr>
<td>arp</td>
<td>640</td>
<td>1</td>
</tr>
<tr>
<td>Command</td>
<td>Rate</td>
<td>Burst</td>
</tr>
<tr>
<td>---------------</td>
<td>------</td>
<td>-------</td>
</tr>
<tr>
<td>dhcp</td>
<td>128</td>
<td>0</td>
</tr>
<tr>
<td>rip</td>
<td>64</td>
<td>1</td>
</tr>
<tr>
<td>ldp</td>
<td>512</td>
<td>1</td>
</tr>
<tr>
<td>ospf</td>
<td>256</td>
<td>1</td>
</tr>
<tr>
<td>pim</td>
<td>128</td>
<td>1</td>
</tr>
<tr>
<td>vrrp</td>
<td>512</td>
<td>1</td>
</tr>
<tr>
<td>rsvp</td>
<td>512</td>
<td>1</td>
</tr>
<tr>
<td>ipda</td>
<td>1024</td>
<td>0</td>
</tr>
<tr>
<td>icmp-redirect</td>
<td>128</td>
<td>0</td>
</tr>
<tr>
<td>mcast-rpf-fail</td>
<td>128</td>
<td>1</td>
</tr>
<tr>
<td>macsa-mismatch</td>
<td>128</td>
<td>0</td>
</tr>
<tr>
<td>port-security-discard</td>
<td>128</td>
<td>0</td>
</tr>
<tr>
<td>vlan-security-discard</td>
<td>128</td>
<td>0</td>
</tr>
<tr>
<td>mtu-dontfrag</td>
<td>64</td>
<td>0</td>
</tr>
<tr>
<td>mtu-frag</td>
<td>64</td>
<td>0</td>
</tr>
<tr>
<td>ptp</td>
<td>512</td>
<td>2</td>
</tr>
<tr>
<td>ip-option</td>
<td>512</td>
<td>0</td>
</tr>
<tr>
<td>ucast-ttl-fail</td>
<td>64</td>
<td>0</td>
</tr>
<tr>
<td>mpls-ttl-fail</td>
<td>64</td>
<td>0</td>
</tr>
<tr>
<td>igmp</td>
<td>128</td>
<td>2</td>
</tr>
<tr>
<td>sflow-ingress</td>
<td>128</td>
<td>0</td>
</tr>
<tr>
<td>sflow-egress</td>
<td>128</td>
<td>0</td>
</tr>
<tr>
<td>fwd-to-cpu</td>
<td>64</td>
<td>0</td>
</tr>
<tr>
<td>mpls-tp-pwoam</td>
<td>128</td>
<td>2</td>
</tr>
</tbody>
</table>

Total rate: 2048 (pps)

Related Commands

### 2.1.27 show processes cpu sorted

**Command Purpose**

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

**Command Syntax**

`show process cpu sorted`

**Command Mode**

Privileged EXEC
Default

None

Usage

None

Examples

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

Switch# show processes cpu sorted

<table>
<thead>
<tr>
<th>PID</th>
<th>TIME</th>
<th>%CPU</th>
<th>TTY</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>924</td>
<td>00:20:03</td>
<td>2.0</td>
<td>?</td>
<td>hsrvd</td>
</tr>
<tr>
<td>956</td>
<td>00:07:17</td>
<td>0.7</td>
<td>?</td>
<td>nsm</td>
</tr>
<tr>
<td>1007</td>
<td>00:02:44</td>
<td>0.2</td>
<td>?</td>
<td>imi</td>
</tr>
<tr>
<td>959</td>
<td>00:01:24</td>
<td>0.1</td>
<td>?</td>
<td>snmpd</td>
</tr>
<tr>
<td>1317</td>
<td>00:00:01</td>
<td>0.1</td>
<td>pts/0</td>
<td>imish</td>
</tr>
<tr>
<td>5</td>
<td>00:00:45</td>
<td>0.0</td>
<td>?</td>
<td>events/0</td>
</tr>
<tr>
<td>983</td>
<td>00:00:23</td>
<td>0.0</td>
<td>?</td>
<td>mstpd</td>
</tr>
<tr>
<td>985</td>
<td>00:00:15</td>
<td>0.0</td>
<td>?</td>
<td>onmd</td>
</tr>
<tr>
<td>966</td>
<td>00:00:15</td>
<td>0.0</td>
<td>?</td>
<td>lacpd</td>
</tr>
<tr>
<td>963</td>
<td>00:00:12</td>
<td>0.0</td>
<td>?</td>
<td>bhm</td>
</tr>
<tr>
<td>929</td>
<td>00:00:12</td>
<td>0.0</td>
<td>?</td>
<td>chsm</td>
</tr>
<tr>
<td>964</td>
<td>00:00:11</td>
<td>0.0</td>
<td>?</td>
<td>oamd</td>
</tr>
<tr>
<td>919</td>
<td>00:00:10</td>
<td>0.0</td>
<td>?</td>
<td>ntpd</td>
</tr>
<tr>
<td>1003</td>
<td>00:00:08</td>
<td>0.0</td>
<td>?</td>
<td>pimd</td>
</tr>
<tr>
<td>942</td>
<td>00:00:08</td>
<td>0.0</td>
<td>?</td>
<td>sshd</td>
</tr>
<tr>
<td>957</td>
<td>00:00:08</td>
<td>0.0</td>
<td>?</td>
<td>dhcrelay</td>
</tr>
<tr>
<td>973</td>
<td>00:00:07</td>
<td>0.0</td>
<td>?</td>
<td>authd</td>
</tr>
<tr>
<td>1005</td>
<td>00:00:07</td>
<td>0.0</td>
<td>?</td>
<td>ldpd</td>
</tr>
<tr>
<td>977</td>
<td>00:00:07</td>
<td>0.0</td>
<td>?</td>
<td>rmond</td>
</tr>
<tr>
<td>1021</td>
<td>00:00:07</td>
<td>0.0</td>
<td>?</td>
<td>ripd</td>
</tr>
<tr>
<td>1027</td>
<td>00:00:07</td>
<td>0.0</td>
<td>?</td>
<td>ospfd</td>
</tr>
<tr>
<td>1032</td>
<td>00:00:07</td>
<td>0.0</td>
<td>?</td>
<td>bgpd</td>
</tr>
<tr>
<td>1003</td>
<td>00:00:05</td>
<td>0.0</td>
<td>?</td>
<td>init</td>
</tr>
<tr>
<td>779</td>
<td>00:00:04</td>
<td>0.0</td>
<td>?</td>
<td>jffs2_gcd_mtd1</td>
</tr>
<tr>
<td>1106</td>
<td>00:00:01</td>
<td>0.0</td>
<td>?</td>
<td>imish</td>
</tr>
<tr>
<td>3</td>
<td>00:00:00</td>
<td>0.0</td>
<td>?</td>
<td>ksoftirqd/0</td>
</tr>
<tr>
<td>916</td>
<td>00:00:00</td>
<td>0.0</td>
<td>?</td>
<td>syslog-ng</td>
</tr>
<tr>
<td>65</td>
<td>00:00:00</td>
<td>0.0</td>
<td>?</td>
<td>bdi-default</td>
</tr>
<tr>
<td>965</td>
<td>00:00:00</td>
<td>0.0</td>
<td>?</td>
<td>ptpd</td>
</tr>
<tr>
<td>917</td>
<td>00:00:00</td>
<td>0.0</td>
<td>?</td>
<td>crond</td>
</tr>
</tbody>
</table>
Related Commands

None

2.1.28 show processes cpu history

Command Purpose

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

Command Syntax

show process cpu history

Command Mode

Privileged EXEC
**Default**

None

**Usage**

None

**Examples**

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

```
Switch# show processes cpu history
CPU usage for five seconds: 4.17%; one minute: 3.70%; five minutes: 3.68%
```

**Related Commands**

None

### 2.1.29 show processes memory sorted

**Command Purpose**

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

**Command Syntax**

```
show processes memory sorted (core | physical | virtual)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>core</td>
<td>Size in physical pages of the core image of the process</td>
<td>-</td>
</tr>
<tr>
<td>physical</td>
<td>Non-swapped physical memory that a task has used</td>
<td>-</td>
</tr>
<tr>
<td>virtual</td>
<td>Virtual memory usage of entire process</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None
## Usage

None

## Examples

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

```sh
Switch# show processes memory sorted

Total: 256108; Used: 89644; Free: 166464; Buffers: 0

<table>
<thead>
<tr>
<th>PID</th>
<th>TTY</th>
<th>RSS</th>
<th>VSZ</th>
<th>SZ</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>1317</td>
<td>pts/0</td>
<td>9516</td>
<td>13104</td>
<td>3276</td>
<td>imish</td>
</tr>
<tr>
<td>1106</td>
<td>?</td>
<td>9428</td>
<td>13104</td>
<td>3276</td>
<td>imish</td>
</tr>
<tr>
<td>1463</td>
<td>pts/0</td>
<td>7436</td>
<td>13104</td>
<td>3276</td>
<td>imish</td>
</tr>
<tr>
<td>956</td>
<td>?</td>
<td>6836</td>
<td>14644</td>
<td>3661</td>
<td>nsm</td>
</tr>
<tr>
<td>1007</td>
<td>?</td>
<td>5948</td>
<td>9624</td>
<td>2406</td>
<td>imi</td>
</tr>
<tr>
<td>924</td>
<td>?</td>
<td>5912</td>
<td>17652</td>
<td>4413</td>
<td>hsrvd</td>
</tr>
<tr>
<td>959</td>
<td>?</td>
<td>3336</td>
<td>8076</td>
<td>2019</td>
<td>snmpd</td>
</tr>
<tr>
<td>1032</td>
<td>?</td>
<td>2724</td>
<td>8204</td>
<td>2051</td>
<td>bgpd</td>
</tr>
<tr>
<td>1027</td>
<td>?</td>
<td>2488</td>
<td>7140</td>
<td>1785</td>
<td>ospfd</td>
</tr>
<tr>
<td>1003</td>
<td>?</td>
<td>2472</td>
<td>7152</td>
<td>1788</td>
<td>pimd</td>
</tr>
<tr>
<td>957</td>
<td>?</td>
<td>2340</td>
<td>6572</td>
<td>1643</td>
<td>dhcpelay</td>
</tr>
<tr>
<td>983</td>
<td>?</td>
<td>2336</td>
<td>6592</td>
<td>1648</td>
<td>mstpd</td>
</tr>
<tr>
<td>1021</td>
<td>?</td>
<td>2324</td>
<td>6600</td>
<td>1650</td>
<td>ripd</td>
</tr>
<tr>
<td>1005</td>
<td>?</td>
<td>2320</td>
<td>6732</td>
<td>1683</td>
<td>ldpd</td>
</tr>
<tr>
<td>942</td>
<td>?</td>
<td>2284</td>
<td>6772</td>
<td>1693</td>
<td>sshd</td>
</tr>
<tr>
<td>985</td>
<td>?</td>
<td>2208</td>
<td>6592</td>
<td>1648</td>
<td>onmd</td>
</tr>
<tr>
<td>929</td>
<td>?</td>
<td>2132</td>
<td>7168</td>
<td>1792</td>
<td>chsm</td>
</tr>
<tr>
<td>966</td>
<td>?</td>
<td>2028</td>
<td>6140</td>
<td>1535</td>
<td>lacpd</td>
</tr>
<tr>
<td>973</td>
<td>?</td>
<td>2028</td>
<td>6284</td>
<td>1571</td>
<td>authd</td>
</tr>
<tr>
<td>965</td>
<td>?</td>
<td>2024</td>
<td>6408</td>
<td>1602</td>
<td>ptpd</td>
</tr>
<tr>
<td>964</td>
<td>?</td>
<td>1952</td>
<td>6364</td>
<td>1591</td>
<td>oamd</td>
</tr>
<tr>
<td>977</td>
<td>?</td>
<td>1948</td>
<td>6200</td>
<td>1550</td>
<td>momd</td>
</tr>
<tr>
<td>963</td>
<td>?</td>
<td>1708</td>
<td>5980</td>
<td>1495</td>
<td>bhm</td>
</tr>
<tr>
<td>919</td>
<td>?</td>
<td>1120</td>
<td>3792</td>
<td>948</td>
<td>ntpd</td>
</tr>
<tr>
<td>916</td>
<td>?</td>
<td>1060</td>
<td>2300</td>
<td>575</td>
<td>syslog-ng</td>
</tr>
<tr>
<td>1465</td>
<td>pts/0</td>
<td>764</td>
<td>2516</td>
<td>629</td>
<td>ps</td>
</tr>
<tr>
<td>917</td>
<td>?</td>
<td>668</td>
<td>3040</td>
<td>760</td>
<td>cron</td>
</tr>
<tr>
<td>1</td>
<td>?</td>
<td>656</td>
<td>2928</td>
<td>732</td>
<td>init</td>
</tr>
<tr>
<td>1464</td>
<td>pts/0</td>
<td>472</td>
<td>1668</td>
<td>417</td>
<td>more</td>
</tr>
<tr>
<td>1096</td>
<td>?</td>
<td>416</td>
<td>2928</td>
<td>732</td>
<td>telnetd</td>
</tr>
<tr>
<td>1098</td>
<td>?</td>
<td>272</td>
<td>2928</td>
<td>732</td>
<td>telnetd</td>
</tr>
<tr>
<td>912</td>
<td>?</td>
<td>172</td>
<td>1496</td>
<td>374</td>
<td>angel</td>
</tr>
<tr>
<td>2</td>
<td>?</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>kthreadd</td>
</tr>
</tbody>
</table>
```
Related Commands

None

2.1.30 terminal monitor

Command Purpose

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

Command Syntax

terminal monitor
terminal no monitor

Command Mode

Privileged EXEC

Default

None
Usage

None

Examples

The following is sample output from the terminal monitor command:

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

Related Commands

None

2.1.31 configure terminal

Command Purpose

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

Command Syntax

configure terminal

Command Mode

Privileged EXEC

Default

None

Usage

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

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

Examples

In the following example, the user enters Global Configuration:
Switch# configure terminal
Switch(config)#

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#

**Related Commands**

- enable
- disable

**2.1.32 disable**

**Command Purpose**

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

**Command Syntax**

disable

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

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

```
Switch# configure terminal
Switch> enable
Password: <password>
Switch# disable
Switch>
```
Related Commands

Enable

2.1.33 enable

Command Purpose

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

Command Syntax

enable

Command Mode

User EXEC
Privileged EXEC

Default

None

Usage

None

Examples

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

Switch# configure terminal
Switch> enable
Password: <password>
Switch# disable
Switch>

Related Commands

Disable
2.1.34 end

Command Purpose

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

Command Syntax

end

Command Mode

Global Configuration

Default

None

Usage

This command will bring you back to Privileged EXEC mode regardless of what configuration mode or configuration sub-mode you are in. This global configuration command can be used in any configuration mode. Use this command when you are done configuring the system and you want to return to EXEC mode to perform verification steps.

Examples

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

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

Related Commands

Exit

2.1.35 exit (global)

Command Purpose

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

exit

Command Mode

All Configuration Mode

Default

None

Usage

The exit command is used in the CLI to exit from the current command mode to the lower mode in the CLI mode hierarchy. For example, use the exit command in Global Configuration to return to Privileged EXEC mode. Use the exit command in interface, line or router configuration mode to return to Global Configuration.

Examples

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

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

Related Commands

end
exit (EXEC)

2.1.36 exit (EXEC)

Command Purpose

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

Command Syntax

exit

Command Mode

Privileged EXEC
Default

None

Usage

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

Examples

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

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

Related Commands

Quit

2.1.37 quit

Command Purpose

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

Command Syntax

```
quit
```

Command Mode

All Configuration Mode

Default

None
Usage

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

Examples

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

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

Related Commands

Exit

2.1.38 cd

Command Purpose

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

Command Syntax

```
cd ( dir )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dir</td>
<td>(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</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

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

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

Examples

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

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

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

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

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

Switch# cd udisk:

% Failed to cd udisk: No such file or directory

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

Related Commands

dir
ls
Pwd

2.1.39 copy

Command Purpose

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

Command Syntax

copy source-name destination-name
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>source-name</td>
<td>The location URL of the source file to be copied. The source can be either local or remote</td>
<td>-</td>
</tr>
<tr>
<td>destination-name</td>
<td>The destination URL of the copied file. The destination can be either local or remote</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

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

**Examples**

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

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

Download from URL to temporary file.

Get file from tftp://192.168.0.1/image

```
+-------------------------------------------------------------+
| Received 15591515 bytes in 16.6 seconds                     |
+-------------------------------------------------------------+
```

Copy the temporary file to its destination.

```
+-------------------------------------------------------------+
| 15591515 bytes in 69.8 seconds, 218 kbytes/second            |
+-------------------------------------------------------------+
```

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

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

**Related Commands**

Delete

2.1.40 delete

**Command Purpose**

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

`delete file-name`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>file-name</td>
<td>The file name that is supposed to be deleted</td>
<td></td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

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

**Examples**

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

Switch# delete flash:/test

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

**Related Commands**

Copy

**2.1.41 dir**

**Command Purpose**

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

**Command Syntax**

dir (flash: | udisk: | directory-name |) ( file-name |)
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>flash</td>
<td>The flash system</td>
<td>-</td>
</tr>
<tr>
<td>udisk</td>
<td>The USB mass storage device. If you don't use USB mass storage device, failed to dir udisk</td>
<td>-</td>
</tr>
<tr>
<td>directory-name</td>
<td>The directory in flash or udisk</td>
<td>-</td>
</tr>
<tr>
<td>file-name</td>
<td>The file name</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

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

**Examples**

The following is sample output from the dir command:

Switch# dir

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

Switch# cd udisk:

Switch# dir

```
Directory of udisk:
total 12
drwxrwxrwx 2 4096 Jun 2 2011 test
drwxrwxrwx 2 4096 Jun 8 2011 test1
drwxrwxrwx 2 4096 Jun 7 2011 test2
3.7G bytes total (3.7G bytes free)
```
The following is sample output from udisk if plug in the USB mass storage device:

```
Switch# cd udisk:
Switch# dir

Directory of udisk/

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

**Related Commands**

Is

**2.1.42 Is**

**Command Purpose**

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

**Command Syntax**

```
Is ( flash: | udisk: | ) ( directory-name | ) ( file-name | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>flash</td>
<td>The flash system</td>
<td>-</td>
</tr>
<tr>
<td>udisk</td>
<td>The USB mass storage device, if you don't use USB mass storage device, failed to dir udisk</td>
<td>-</td>
</tr>
<tr>
<td>directory-name</td>
<td>The directory in flash or udisk</td>
<td>-</td>
</tr>
<tr>
<td>file-name</td>
<td>The file name</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None
Examples

The following is sample output from the ls command:

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

Related Commands

dir

2.1.43 more

Command Purpose

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

Command Syntax

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>flash</td>
<td>The flash system</td>
<td>-</td>
</tr>
<tr>
<td>udisk</td>
<td>The USB mass storage device. If you don't use USB mass storage device, failed to dir udisk</td>
<td>-</td>
</tr>
<tr>
<td>directory-name</td>
<td>The directory in flash or udisk</td>
<td>-</td>
</tr>
<tr>
<td>file-name</td>
<td>The file name</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None
Usage

The system can only display a file in ASCII format.

Examples

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

Switch# more flash:/startup-config.conf

Related Commands

dir
ls

2.1.44 mkdir

Command Purpose

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

Command Syntax

mkdir directory-name

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>directory-name</td>
<td>The directory in flash or udisk</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

This command is valid only for local file systems.

Examples

The following example creates a directory named newdir in Flash:

Switch# mkdir flash:/newdir

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

Switch# mkdir udisk:/newdir
Related Commands

rmdir
dir

2.1.45 rename

Command Purpose

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

Command Syntax

rename old-filename new-filename

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>old-filename</td>
<td>The original file name in flash</td>
<td>-</td>
</tr>
<tr>
<td>new-filename</td>
<td>The new file name in flash</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

This command is valid only for local file systems

Examples

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

Switch# configure terminal
Switch1# rename udisk:/wus udisk:/wu
Are you sure to rename udisk:/wus? [confirm]

Related Commands
2.1.46  rmdir

Command Purpose

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

Command Syntax

rmdir directory-name

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>directory-name</td>
<td>The directory in flash</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

This command is valid only for local file systems

Examples

The following example deletes a directory named newdir:

Switch# rmdir flash:/newdir
Are you sure to delete newdir? [yes/no]: y

Related Commands

mkdir
dir

2.1.47  tar create

Command Purpose

To create a 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>tar-file-name</td>
<td>The file name of the new tar file</td>
<td>-</td>
</tr>
<tr>
<td>source-directory</td>
<td>The source directory in flash</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

The source-directory must be a directory

**Examples**

The following example creates a tar file named tar1:

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

**Related Commands**

- tar table
- tar xtract

**2.1.48 tar table**

**Command Purpose**

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

**Command Syntax**

```
tar table tar-file-name
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>tar-file-name</td>
<td>The file name of the new tar file</td>
<td>-</td>
</tr>
</tbody>
</table>
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:/tar

Related Commands

tar create

2.1.49 tar xtract

Command Purpose

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

Command Syntax

tar xtract tar-file destination-directory

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>tar-file</td>
<td>The file name of the tar file</td>
<td>-</td>
</tr>
<tr>
<td>destination-directory</td>
<td>The destination directory</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None
Usage

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

Examples

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

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

Related Commands

tar create
tar table

2.1.50  show diagnostic-information

Command Purpose

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

Command Syntax

show diagnostic-information ( bgp | ospf )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp</td>
<td>BGP protocol diagnostic information</td>
<td>-</td>
</tr>
<tr>
<td>ospf</td>
<td>OSPF protocol diagnostic information</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example show diagnostic-information:

Switch# show diagnostic-information
Related Commands

None

2.1.51 tar diagnostic-information

Command Purpose

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

Command Syntax

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination-directory</td>
<td>The destination directory, such as flash, udisk, tftp or ftp server</td>
<td>-</td>
</tr>
<tr>
<td>tar-file</td>
<td>The file name of the tar file</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

The destination-directory must reachable and disk is enough

Examples

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

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

Related Commands

None
2.1.52 format

Command Purpose

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

Command Syntax

format udisk:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>udisk</td>
<td>The USB mass storage device. If you don’t use USB mass storage device, failed to format udisk</td>
<td>–</td>
</tr>
</tbody>
</table>

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

2.1.53 umount

Command Purpose

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

umount udisk:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>udisk:</td>
<td>The USB mass storage device. If you don’t use USB mass storage device, failed to format udisk</td>
<td>-</td>
</tr>
</tbody>
</table>

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

2.1.54 cut-through enable

Command Purpose

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

Command Syntax

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

no cut_through_forwarding enable
### Command Mode

**Application Configuration**

**Default**

10G-40G-100G

**Usage**

None

**Examples**

The following example shows how to configure cut through mode:

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

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

**Related Commands**

None

#### 2.1.55 show cut-through-forwarding mode

**Command Purpose**

To display current working mode.

**Command Syntax**

show cut-through-forwarding mode

**Command Mode**

Privileged EXEC
Default

None

Usage

None

Examples

The following shows an example to display current working mode:

DUT1# show cut-through-forwarding mode

Related Commands

2.1.56 reset factory-config

Command Purpose

Reset to factory configuration.

Command Syntax

reset factory-config

Command Mode

Privileged EXEC

Default

None

Usage

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

Examples

The following shows an example to reset factory configuration:

Switch# configure terminal
DUT1# reset factory-config
This action will reset the saved configuration immediately. Running-config will be erased after reboot. Continue? [yes/no]:

Related Commands

2.1.57  show factory-config

Command Purpose

To display the factory configuration.

Command Syntax

show factory-config

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

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

DUT1# show factory-config

Related Commands

2.1.58  show this

Command Purpose

To display the configuration of this mode.

Command Syntax

show this
**Command Mode**

All Configuration Mode

**Default**

None

**Usage**

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

**Examples**

The following example show the configuration of this mode:

Switch(config-vlan)# show this

```
vlan database
  vlan 5
! 
```

**Related Commands**

None

**2.1.59 show route-mac**

**Command Purpose**

To display the route MAC address of this device.

**Command Syntax**

show route-mac

**Command Mode**

Privileged EXEC

**Default**

None
Usage

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

Examples

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

```
Switch# show route-mac
Route MAC is: 222c.12fd.6c00
```

Related Commands

None

2.2 User Management Commands

2.2.1 username

Command Purpose

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

Command Syntax

```
username WORD
no username WORD
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>Establish User Name Authentication</td>
<td>-</td>
</tr>
<tr>
<td>WORD</td>
<td>User name</td>
<td>-</td>
</tr>
</tbody>
</table>

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

2.2.2 username password

Command Purpose

Use this command to add username and password.

Command Syntax

```
username WORD password (8 | ) LINE
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>User name</td>
<td>-</td>
</tr>
<tr>
<td>Password</td>
<td>Password for username</td>
<td>-</td>
</tr>
<tr>
<td>(8)</td>
<td>Specifies a hidden password will follow</td>
<td>-</td>
</tr>
<tr>
<td>LINE</td>
<td>User password string</td>
<td>-</td>
</tr>
</tbody>
</table>

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
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>User name</td>
<td>-</td>
</tr>
<tr>
<td>secret</td>
<td>Specify the secret for the user</td>
<td>-</td>
</tr>
<tr>
<td>LINE</td>
<td>User privilege level</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

None

Examples

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

Switch# configure terminal
Switch(config)#username testName secret 123456

Related Commands

2.2.4 username privilege

Command Purpose

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

Command Syntax

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

**Command Mode**

**Global Configuration**

**Default**

None

**Usage**

None

**Examples**

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

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

**Related Commands**

**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 | -

**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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>User name</td>
<td>-</td>
</tr>
<tr>
<td>privilege &lt;1-4&gt;</td>
<td>User privilege level</td>
<td>-</td>
</tr>
<tr>
<td>8</td>
<td>Specifies a HIDDEN password will follow</td>
<td>-</td>
</tr>
<tr>
<td>LINE</td>
<td>User privilege level</td>
<td>-</td>
</tr>
</tbody>
</table>

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

2.2.7 re-username newname

Command Purpose

Use this command to reset username.

Command Syntax

re-username WORD newname WORD

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>re-username WORD</td>
<td>Old user name</td>
<td>-</td>
</tr>
<tr>
<td>newname WORD</td>
<td>New user name</td>
<td>-</td>
</tr>
</tbody>
</table>

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
2.2.8 cipher detect

Command Purpose

Use this command to set high level of cipher detect.

Command Syntax

cipher detect (strong | normal | none)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>strong</td>
<td>Cipher must contain digital, normal char and special char</td>
<td>-</td>
</tr>
<tr>
<td>normal</td>
<td>Cipher must contain digital and normal char</td>
<td>-</td>
</tr>
<tr>
<td>none</td>
<td>Disable security check</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

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

Examples

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

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

Related Commands

2.3 FTP Commands

2.3.1 ftp

Command Purpose

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

`ftp (mgmt-if | ) host`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt-if</td>
<td>Management port</td>
<td>-</td>
</tr>
<tr>
<td>HOST</td>
<td>IPv4, IPv6 address or name of the remote host</td>
<td>Support IPv4/IPv6 address or hostname</td>
</tr>
</tbody>
</table>

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

Related Commands

2.3.2 ftp vrf

Command Purpose

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

Command Syntax

ftp vrf WORD

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>VPN Routing/Forwarding instance name</td>
<td>A string with 1-15 characters</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

Switch# ftp vrf testvrf

Related Commands
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>USERNAME</td>
<td>The user name of the remote FTP server</td>
<td>Up to 31 characters</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LINE</td>
<td>The password of the user name of the remote FTP server</td>
<td>Up to 128 characters</td>
</tr>
<tr>
<td>8</td>
<td>Specifies a hidden password will follow</td>
<td>-</td>
</tr>
</tbody>
</table>

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

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

Privileged EXEC

Default

None

Usage

None

Examples

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

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

Related Commands

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

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

Command Mode

Privileged EXEC

Default

None
Usage

None

Examples

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

```
Switch# copy ftp://username:password@1.1.1.1:21/test.c flash:test1.c
get file from ftp://username:password@1.1.1.1:21/test.c
.
Received 225 bytes in 0.3 seconds
```

Related Commands

2.4 TFTP Commands

2.4.1 copy GFFILENAME GURLNNAME

Command Purpose

Use this command to copy local file to tftp server.

Command Syntax

```
copy GFFILENAME ( vrf VRF_NAME | ) ( mgmt-if | -a SRC_ADDR | -si SRC_INTF ) GURLNNAME
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt-if</td>
<td>Management port</td>
<td>-</td>
</tr>
<tr>
<td>vrf WORD</td>
<td>VPN Routing/Forwarding instance</td>
<td>A string with 1-15 characters</td>
</tr>
<tr>
<td>GFFILENAME</td>
<td>Copy from local file</td>
<td>The full path and file name, up to 255 characters</td>
</tr>
<tr>
<td>GURLNNAME</td>
<td>Copy to local file</td>
<td>The full path and file name, up to 255 characters</td>
</tr>
<tr>
<td>-a SRC_ADDR</td>
<td>Copy with assigned IP</td>
<td>-</td>
</tr>
<tr>
<td>-si SRC_INTF</td>
<td>Copy with assigned Interface</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None
Usage

None

Examples

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

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

Related Commands

2.4.2 copy GURLNAME GFILNENAME

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 GFILNENAME`

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

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>startup-config</td>
<td>Copy from current system configuration</td>
<td>-</td>
</tr>
<tr>
<td>mgmt-if</td>
<td>Management port</td>
<td>-</td>
</tr>
<tr>
<td>GURLNAME</td>
<td>Copy to URL</td>
<td>The full path and file name, up to 255 characters</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt-if</td>
<td>Management port</td>
<td>-</td>
</tr>
<tr>
<td>GURLNAME</td>
<td>Copy from URL</td>
<td>The full path and file name, up to 255 characters</td>
</tr>
<tr>
<td>startup-config</td>
<td>Copy to startup system configuration</td>
<td>-</td>
</tr>
</tbody>
</table>

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
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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt-if</td>
<td>Management port</td>
<td>-</td>
</tr>
<tr>
<td>GFilename</td>
<td>Copy from local file</td>
<td>The full path and file name, up to 255 characters</td>
</tr>
<tr>
<td>Gurlname</td>
<td>Copy to local file</td>
<td>The full path and file name, up to 255 characters</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

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

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

Related Commands

2.5.2 copy Gurlname GFilename

Command Purpose

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

`copy ( mgmt-if | ) GURLNAME GFFILENAME`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt-if</td>
<td>Management port</td>
<td>-</td>
</tr>
<tr>
<td>GURLNAME</td>
<td>Copy from URL</td>
<td>The full path and file name, up to 255 characters</td>
</tr>
<tr>
<td>GFFILENAME</td>
<td>Copy to local file</td>
<td>The full path and file name, up to 255 characters</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

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

```
Switch# copy scp://1.1.1.1/test.c flash:test1.c
get file from scp://1.1.1.1/test.c
Received 225 bytes in 0.3 seconds
```

Related Commands

2.5.3 `copy running-config mgmt-if`

Command Purpose

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

Command Syntax

`copy running-config ( mgmt-if | ) GURLNAME`
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>startup-config</td>
<td>Copy from current system configuration</td>
<td>-</td>
</tr>
<tr>
<td>mgmt-if</td>
<td>Management port</td>
<td>-</td>
</tr>
<tr>
<td>GURLNAME</td>
<td>Copy to URL</td>
<td>The full path and file name, up to 255 characters</td>
</tr>
</tbody>
</table>

**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**

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`
### 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**

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

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

2.6.2 ip telnet server source address

Command Purpose

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

Command Syntax

ip telnet server source address (vrf NAME) IP_ADDR
no ip telnet server source address

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf NAME</td>
<td>Specify a vrf to provide telnet server</td>
<td>A string with 1-15 characters</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>Configure IP address for telnet server working inband</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

**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:

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

**Related Commands**

2.6.3 ip telnet server source port

**Command Purpose**

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

**Command Syntax**

```
ip telnet server source port NUMBER
```

no ip telnet server source port

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>port NUMBER</td>
<td>Configure TCP port for telnet server working inband</td>
<td>1025-65535</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration
Default

None

Usage

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

Examples

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

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

Related Commands

2.6.4 ip telnet server source mgmt-if port

Command Purpose

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

Command Syntax

ip telnet server source mgmt-if port NUMBER
no ip telnet server source mgmt-if port

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt-if port NUMBER</td>
<td>Configure TCP port for telnet server working outband</td>
<td>1025-65535</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

The CLI of “no telnet server source 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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip telnet server source mgmt-if port 2323</td>
<td></td>
</tr>
</tbody>
</table>

Related Commands

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)`

Command Mode

Global Configuration

Default

SSH service is enabled.

Usage

None

Examples

The following example enables the SSH service on your switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip ssh server enable</td>
<td></td>
</tr>
</tbody>
</table>

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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>COUNT</td>
<td>The number of retries, with a maximum of 6 authentication retries</td>
<td>1-6</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>The number of seconds until timeout disconnects</td>
<td>1-120 seconds</td>
</tr>
</tbody>
</table>

### Command Mode

Global Configuration

### Default

The default is 120 seconds.

### Usage

None

### Examples

The following examples configure SSH authentication timeout on your switch:

```bash
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

```bash
ip ssh server authentication-type (all | (password | public-key | rsa))
no ip ssh server authentication-type
```
### 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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEYNAME</td>
<td>The key value for host key</td>
<td>Up to 32 characters</td>
</tr>
</tbody>
</table>
Command Mode

Global Configuration

Default

None

Usage

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

Examples

The following examples configure SSH host key on your switch:

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

Related Commands

show ip ssh server status

2.7.6 ip ssh server rekey-interval

Command Purpose

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

Command Syntax

ip ssh server rekey-interval MINUTE
no ip ssh server rekey-interval

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MINUTE</td>
<td>The rekey interval in minutes</td>
<td>1-1440 minutes</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Switch runs only SSH Version 1</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>Switch runs only SSH Version 2</td>
<td>-</td>
</tr>
<tr>
<td>all</td>
<td>Version 1 and Version 2 are both supported</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

The default SSH version is 2.

Usage

You can use this command with the 2 keywords 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf NAME</td>
<td>Specify a vrf to provide SSH server</td>
<td>Up to 15 characters</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>Configure IP address for SSH server working inband</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>port NUMBER</td>
<td>Configure TCP port for SSH server working inband</td>
<td>1025-65535</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt-if port</td>
<td>Configure TCP port for SSH server working outband</td>
<td>1025-65535</td>
</tr>
</tbody>
</table>

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
```

<table>
<thead>
<tr>
<th>Version</th>
<th>Encryption</th>
<th>Hmac</th>
<th>User</th>
<th>IP</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>aes128-cbc</td>
<td>hmac-md5</td>
<td>abc</td>
<td>10.10.29.22</td>
<td>Session started</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEYNAME</td>
<td>The name of the key</td>
<td>Up to 32 characters</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEYNAME</td>
<td>The name of the key</td>
<td>Up to 32 characters</td>
</tr>
</tbody>
</table>

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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>der</td>
<td>The format is der</td>
<td>-</td>
</tr>
<tr>
<td>pem</td>
<td>The format is pem</td>
<td>-</td>
</tr>
</tbody>
</table>

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-rsa-key)#

Related Commands

csa 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 )
### 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>public</td>
<td>Specify the key as a public key</td>
<td>-</td>
</tr>
<tr>
<td>private</td>
<td>Specify the key as a private key</td>
<td>-</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEYLINE</td>
<td>key line</td>
<td>key line string</td>
</tr>
</tbody>
</table>

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 9DAD748 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)

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

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 )

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEYNAME</td>
<td>Specify the key name to display</td>
<td>Up to 32 characters</td>
</tr>
</tbody>
</table>

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
983E9726 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 )
```

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

Command Mode

Privileged EXEC

Default

None
Usage

None

Examples

The following example displays the usage of this command:

Switch# ssh -I 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

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

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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZONE</td>
<td>Specify the zone name</td>
<td>the length should be (3, 32), and only [a-zA-Z_] is supported, and the first and last character must be alphabet.</td>
</tr>
<tr>
<td>add</td>
<td>Specify the time offset is positive from UTC</td>
<td>-</td>
</tr>
<tr>
<td>minus</td>
<td>Specify the time offset is negative from UTC</td>
<td>-</td>
</tr>
<tr>
<td>HOUR_OFFSET</td>
<td>Specify the time offset in hours</td>
<td>0-23</td>
</tr>
<tr>
<td>MINUTES_OFFSET</td>
<td>[optional]Specify the time offset in minutes, should be in range 0 to 59</td>
<td>0-59</td>
</tr>
<tr>
<td>SECCONDS_OFFSET</td>
<td>[optional]Specify the time offset in seconds</td>
<td>0-59</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZONE</td>
<td>Specify the summer zone name</td>
<td>The length should be [3, 32), and only [a-zA-Z_] is supported, and the first and last character must be alphabet.</td>
</tr>
<tr>
<td>recurring</td>
<td>Specify that summer time starts and ends on a particular day of the week each year</td>
<td>-</td>
</tr>
<tr>
<td>date</td>
<td>Specify that summer time starts and ends on a particular day of the specified year</td>
<td>-</td>
</tr>
<tr>
<td>START_TIME</td>
<td>Specify the start time of summer time</td>
<td>For recurring summer time, the format should be month, day, hh:mm:ss or (first</td>
</tr>
<tr>
<td>END_TIME</td>
<td>Specify the end time of summer time</td>
<td>For recurring summer time, the format should be month, day, hh:mm:ss or (first</td>
</tr>
<tr>
<td>OFFSET</td>
<td>For offset, specify the number of minutes to add during summer time. The default is 60.</td>
<td>1-1440 minutes</td>
</tr>
</tbody>
</table>
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 October 31st 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 |
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Display the configured timezone and summer time information in addition to current date and time</td>
<td>-</td>
</tr>
</tbody>
</table>

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 timezones

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 ( GFFILENAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt-if</td>
<td>Management port</td>
<td>-</td>
</tr>
<tr>
<td>GFILENAME</td>
<td>URL name</td>
<td>-</td>
</tr>
<tr>
<td>GFFILENAME</td>
<td>local file name</td>
<td>-</td>
</tr>
</tbody>
</table>

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

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 ( GFFILENAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GFFILENAME</td>
<td>local file name</td>
<td>-</td>
</tr>
</tbody>
</table>

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 license

License files:
======================================================================
Related Commands

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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Turn on the HTTP service</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>Turn off the HTTP service</td>
<td>-</td>
</tr>
</tbody>
</table>

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)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Turn on the HTTPS service</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>Turn off the HTTPS service</td>
<td>-</td>
</tr>
</tbody>
</table>

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, use the http server load command.

Command Syntax

http server load FILENAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>FILENAME</td>
<td>Name of WEB image</td>
<td>-</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIMEOUT</td>
<td>Online web user expire time.</td>
<td>The range is [1,60], unit is minute.</td>
</tr>
</tbody>
</table>

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

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PORT</td>
<td>Configure TCP port for HTTP server working inband</td>
<td>1025-65535</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PORT</td>
<td>Configure TCP port for HTTPS server working inband</td>
<td>1025-65535</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PORT</td>
<td>Configure TCP port for HTTP server working outband</td>
<td>1025-65535</td>
</tr>
</tbody>
</table>
**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PORT</td>
<td>Configure TCP port for HTTPS server working outband</td>
<td>1025-65535</td>
</tr>
</tbody>
</table>

**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 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 ) )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>Configure web login authentication by local</td>
<td>-</td>
</tr>
<tr>
<td>aaa</td>
<td>Configure web login authentication by AAA</td>
<td>-</td>
</tr>
<tr>
<td>login-authentication</td>
<td>Configure web login authentication method list</td>
<td>-</td>
</tr>
<tr>
<td>exec-authorization</td>
<td>Configure web login authorization method list</td>
<td>-</td>
</tr>
<tr>
<td>default</td>
<td>Set method list name default</td>
<td>-</td>
</tr>
<tr>
<td>LISTNAME</td>
<td>Set method list name</td>
<td>Up to 31 characters</td>
</tr>
</tbody>
</table>

**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 | ) ) | disable )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Turn on the RPC-API service</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>Turn off the RPC-API service</td>
<td>-</td>
</tr>
<tr>
<td>PORT</td>
<td>TCP port number. TCP port number. By default, the RPC-API service listens on TCP port 80 (HTTP)</td>
<td>1025-65535</td>
</tr>
<tr>
<td>vrf NAME</td>
<td>VPN Routing/Forwarding instance</td>
<td>A string with 1-15 characters</td>
</tr>
<tr>
<td>ssl</td>
<td>Enable SSL (HTTPS)</td>
<td>-</td>
</tr>
<tr>
<td>SSLPORT</td>
<td>TCP port number. TCP port number. By default, the RPC-API service listens on TCP port 443 (HTTPS)</td>
<td>1025-65535</td>
</tr>
</tbody>
</table>
**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
Chapter 3 Ethernet Commands

3.1 Interface Commands

3.1.1 bandwidth

Command Purpose
Use this command to set the bandwidth of the port.
To return the bandwidth to default value, use the no form of this command.

Command Syntax
bandwidth BANDWIDTH
no bandwidth

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>BANDWIDTH</td>
<td>port bandwidth</td>
<td>1-100000000, unit: kbps</td>
</tr>
</tbody>
</table>

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 | }
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LINE</td>
<td>The description on the interface</td>
<td>should be no more than 240 characters, and the character can not include '?'</td>
</tr>
</tbody>
</table>

**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
```

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

Command Mode

Interface Configuration

Default

Auto

Usage

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

Examples

The following example sets the duplex mode to auto:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# duplex auto

The following example sets the duplex mode to full:

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

The following example returns the duplex mode to default:

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

**Related Commands**

bandwidth

speed

3.1.5 speed

**Command Purpose**

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

**Command Syntax**

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

```
no speed
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Port automatically detects the speed it should run</td>
<td>-</td>
</tr>
<tr>
<td>10</td>
<td>Port runs at 10 Mb/s</td>
<td>-</td>
</tr>
<tr>
<td>100</td>
<td>Port runs at 100 Mb/s</td>
<td>-</td>
</tr>
<tr>
<td>1000</td>
<td>Port runs at 1000 Mb/s</td>
<td>-</td>
</tr>
<tr>
<td>2G5</td>
<td>Port runs at 2.5Gb/s</td>
<td>-</td>
</tr>
<tr>
<td>5G</td>
<td>Port runs at 5Gb/s</td>
<td>-</td>
</tr>
<tr>
<td>10G</td>
<td>Port runs at 10Gb/s</td>
<td>-</td>
</tr>
<tr>
<td>40G</td>
<td>Port runs at 40Gb/s</td>
<td>-</td>
</tr>
<tr>
<td>100G</td>
<td>Port runs at 100Gb/s</td>
<td>-</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>The name of interface, i.e. eth-0-1, agg1, vlan1, loopback1</td>
<td>Support all interface types</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface range</td>
<td>Support all interface types can be separate by comma, dash</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_RANGE</td>
<td>VLAN ID range</td>
<td>VLAN ID range is 1-4094, can be separate by comma, dash</td>
</tr>
</tbody>
</table>
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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-select</td>
<td>Enable the switch to dynamically select the type based on which one first links up</td>
<td>-</td>
</tr>
<tr>
<td>rj45</td>
<td>Select the RJ-45 interface</td>
<td>-</td>
</tr>
<tr>
<td>sfp</td>
<td>Select the small form-factor pluggable (SFP) module interface</td>
<td>-</td>
</tr>
</tbody>
</table>

**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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable unidirectional function</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>disable unidirectional function</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

disable unidirectional function

**Usage**

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

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

The following example shows how to enable unidirectional function:

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

The following example shows how to disable unidirectional function:

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

Related Commands

3.1.12 shutdown

Command Purpose

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

Command Syntax

```
shutdown
no shutdown
```

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

The following example shows how to shutdown a port:

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

The following example shows how to admin up a port:

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

Related Commands

None

3.1.13 split interface

Command Purpose

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

Command Syntax

```
split interface IFNAME ( 10giga | 40giga )
no split interface
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>the physic port needs to split</td>
<td>Support physical ports</td>
</tr>
<tr>
<td>10giga</td>
<td>split physic port to four 10G port</td>
<td>-</td>
</tr>
<tr>
<td>40giga</td>
<td>split physic port to one 10G port</td>
<td>-</td>
</tr>
</tbody>
</table>
**Command Mode**
Global Configuration

**Default**
None

**Usage**
Need save configuration and reboot to make command take effect

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

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

**Related Commands**
None

---

### 3.1.14 load-interval

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

**Command Syntax**
load-interval SECONDS
no load-interval

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>Load interval</td>
<td>30-600, unit: second</td>
</tr>
</tbody>
</table>

**Command Mode**
Interface Configuration

**Default**
300 seconds

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

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

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

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

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

**Related Commands**
show interface
3.1.15  vlan dot1q tag native

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

Command Syntax
vlan dot1q tag native
no vlan dot1q tag native

Command Mode
Interface Configuration

Default
None

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

Examples
This example shows how to tag native for trunk port:

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

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

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

Related Commands
None

3.1.16  show interface

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

Command Syntax
show interface [ IFNAME ]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
</table>
| 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

3.1.17 show interface status

Command Purpose

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

Command Syntax

show interface (IFNAME) status

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>The interface name</td>
<td>Support aggregation and physical ports</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Duplex</th>
<th>Speed</th>
<th>Mode</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-0-1</td>
<td>down</td>
<td>a-full</td>
<td>a-1000</td>
<td>ACCESS</td>
<td>1000BASE_T_SFP</td>
<td></td>
</tr>
<tr>
<td>eth-0-2</td>
<td>down</td>
<td>a-full</td>
<td>a-1000</td>
<td>ACCESS</td>
<td>1000BASE_T_SFP</td>
<td></td>
</tr>
</tbody>
</table>
### Related Commands

None

#### 3.1.18 show interface summary

**Command Purpose**

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

**Command Syntax**

```
show interface (IFNAME |) summary
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>The interface name</td>
<td>Support all interface types</td>
</tr>
</tbody>
</table>

**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)

<table>
<thead>
<tr>
<th>Interface</th>
<th>Link</th>
<th>RXBS</th>
<th>RXPS</th>
<th>TXBS</th>
<th>TXPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-0-1</td>
<td>DOWN</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

**Related Commands**

show interface

#### 3.1.19 show ip interface

**Command Purpose**

Use this command to show layer3 interface information.
Command Syntax

show ip interface (IFNAME |)
show ip interface brief

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>The interface name, can be eth, vlan or agg</td>
<td>Support all interface types</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC
Default
None

Usage
None

Examples
This example shows the vlan interface information:

```
Switch# show interface vlan10
Interface vlan10
   Interface current state: DOWN
   Hardware is VLAN, address is 8633.d260.6500 (bia 8633.d260.6500)
   Bandwidth 1000000 kbits
   Index 4098 , Metric 1 , Encapsulation ARPA
   The maximum transmit unit (MTU) is 1500 bytes
   VRF binding: not bound
   Label switching is disabled
   No virtual circuit configured
   VRRP master of: VRRP is not configured on this interface
   ARP timeout 01:00:00, ARP retry interval 1s
```

Related Commands
None

3.1.20 switchport

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

Command Syntax

```
switchport
no switchport
```

Command Mode
Interface Configuration

Default
Switchport

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

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

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

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

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

Related Commands

None

3.1.21 switchport access allowed

Command Purpose

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

Command Syntax

```
switchport access allowed vlan (add | remove) VLAN_ID
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Allow the traffic from the vlan to pass the access port</td>
<td>-</td>
</tr>
<tr>
<td>remove</td>
<td>Not allow the traffic from the vlan to pass the access port</td>
<td>-</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>Vlan list connected with '-' and ',' for example, &quot;1-10,15,20,30-40&quot;</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

```
1
```

Usage

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

Examples

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

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

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

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport access allowed vlan add 11
```
This example shows how to refuse the traffic from the vlan12 to pass the port:

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

**Related Commands**

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

### 3.1.22 switchport access vlan

**Command Purpose**

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

**Command Syntax**

```
switchport access vlan VLAN_ID
```

```
o switchport access vlan
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan id</td>
<td>2-4094</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

1

**Usage**

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

**Examples**

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

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

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

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

**Related Commands**

switchport trunk native

### 3.1.23 switchport mode access

**Command Purpose**

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

**Command Syntax**

```
switchport mode access
```

**Command Mode**

Interface Configuration
Default
Access Port

Usage
The access mode is usually used to connect the port to a terminal device, such as a PC.
When the mode is changed, both the MAC learnt dynamically and configured statically on the port will be cleared.

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

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

Related Commands
switchport mode trunk

3.1.24 switchport mode trunk

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

Command Syntax
switchport mode trunk

Command Mode
Interface Configuration

Default
Access Port

Usage
The trunk mode is usually used to connect the port with another switch.
The trunk mode can also be used to connect the port with host device.
When the mode is changed, both the MAC learnt dynamically and configured statically on the port will be cleared.

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

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

Related Commands
switchport mode access

3.1.25 switchport mode dot1q-tunnel

Command Purpose
Use this command to configure the port as QINQ port.

Command Syntax
switchport mode dot1q-tunnel

Command Mode
Interface Configuration


Default
Access Port

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

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

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

Related Commands
switchport mode trunk

3.1.26 switchport trunk allowed

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>add VLAN_ID</td>
<td>allow the traffic from the specified vlan to transmit the trunk port. Vlan list connected with '-', and ',' for example, &quot;1-10,15,20,30-40&quot;</td>
<td>1-4094</td>
</tr>
<tr>
<td>remove VLAN_ID</td>
<td>do not allow the traffic from the specified vlan to transmit the trunk port. Vlan list connected with '-' and ',' for example, &quot;1-10,15,20,30-40&quot;</td>
<td>1-4094</td>
</tr>
<tr>
<td>all</td>
<td>allow the traffic from all the vlan to transmit the trunk port</td>
<td>-</td>
</tr>
<tr>
<td>none</td>
<td>do not allow the traffic from all the vlan to transmit the trunk port</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
1

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

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

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport trunk allowed vlan add 10
This example shows how to refuse traffic from the specified VLAN to transmit the trunk port:

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

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

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

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

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

Related Commands

switchport access allowed vlan (add | remove) vid

3.1.27 switchport trunk native vlan

Command Purpose

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

Command Syntax

switchport trunk native vlan VLAN_ID

no switchport trunk native vlan

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan id</td>
<td>2-4094</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

1

Usage

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

Examples

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

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

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

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

Related Commands

switchport access vlan vid
3.1.28 switchport port-bridge enable

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

**Command Syntax**

```
switchport port-bridge enable
no switchport port-bridge enable
```

**Command Mode**
Interface Configuration

**Default**
None

**Usage**
None

**Examples**
This example shows how to enable port-bridge:

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

**Related Commands**
- port-bridge enable

3.1.29 port-bridge enable

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

**Command Syntax**

```
port-bridge enable
no port-bridge enable
```

**Command Mode**
Global Configuration

**Default**
None

**Usage**
None

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

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

**Related Commands**
- switchport port-bridge enable

3.1.30 port-xconnect

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

port-xconnect destination-interface ( IFPHYSICAL | IFAGG )

no port-xconnect destination-interface

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFPHYSICAL</td>
<td>Physical port</td>
<td>N/A</td>
</tr>
<tr>
<td>IFAGG</td>
<td>Aggregate port</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
None

Usage
None

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

Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface eth-0-1
Switch(config-if)# port-xconnect destination-interface eth-0-2

Related Commands
3.1.31 mtu

Command Purpose
Use this command to configure the maximum transmit unit for this interface.

Command Syntax

mtu VALUE

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VALUE</td>
<td>MTU</td>
<td>68-9216</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>link-flap</td>
<td>Enable detect Link flap error</td>
<td>-</td>
</tr>
<tr>
<td>fdb-flap</td>
<td>Enable detect FDB error</td>
<td>-</td>
</tr>
<tr>
<td>udld</td>
<td>Enable detect UDLD error</td>
<td>-</td>
</tr>
</tbody>
</table>

**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**
```plaintext```
errdisable recovery interval RANGE
no errdisable recovery interval
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RANGE</td>
<td>Recovery interval range</td>
<td>30-86400, unit: second</td>
</tr>
</tbody>
</table>
**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 recover 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>COUNT</td>
<td>Set the FDB-loop times, default 10.</td>
<td>3-50</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_LIST</td>
<td>Set the vlan list that not need FDB-loop detect</td>
<td>Connected with '-' and ':' for example, &quot;1-10,15,20,30-40&quot;</td>
</tr>
</tbody>
</table>

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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enable timer to recover from all reason</td>
<td>-</td>
</tr>
<tr>
<td>bpduguard</td>
<td>Enable timer to recover from BPDU Guard error disable state</td>
<td>-</td>
</tr>
<tr>
<td>bpduloop</td>
<td>Enable timer to recover from BPDU Loopback error disable state</td>
<td>-</td>
</tr>
<tr>
<td>port-security</td>
<td>Enable timer to recover from Port security failure</td>
<td>-</td>
</tr>
<tr>
<td>link-flap</td>
<td>Enable timer to recover from Link flap failure</td>
<td>-</td>
</tr>
<tr>
<td>link-monitor-failure</td>
<td>Enable timer to recover from link monitoring failure</td>
<td>-</td>
</tr>
<tr>
<td>oam-remote-failure</td>
<td>Enable timer to recover from OAM detected remote failure</td>
<td>-</td>
</tr>
<tr>
<td>udld</td>
<td>Enable timer to recover from UDLD failure</td>
<td>-</td>
</tr>
<tr>
<td>fdb-loop</td>
<td>Enable timer to recover from FDB loop failure</td>
<td>-</td>
</tr>
<tr>
<td>loopback-detection</td>
<td>Enable timer to recover from loopback detection error disable state</td>
<td>-</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>link-flap</td>
<td>Configure link flap conditions</td>
<td>-</td>
</tr>
<tr>
<td>COUNT</td>
<td>Max flap count</td>
<td>1-100, unit: times</td>
</tr>
<tr>
<td>SECONDS</td>
<td>Flap count time in seconds</td>
<td>1-120, unit: second</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
count: 10, seconds:10

Usage
Only the link flap can be detected. <1-100> is the threshold of flap count, and <1-120> is the count time in seconds for flap count. If the errdisable detect link flap is enabled, will result in link flap errdisable, otherwise, will only print a message in log.

Examples
This example shows how to set link flap conditions to 20 times in 60 seconds:

Switch# configure terminal
Switch(config)# errdisable flap reason link-flap 20 60

This example shows how to disable link flap conditions to default:

Switch# configure terminal
Switch(config)# no errdisable flap reason link-flap

Related Commands
show errdisable flap

3.2.7 show errdisable detect

Command Purpose
Use this command to display the error disable detection reason.

Command Syntax
showCommand Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to display the error disable detection reason: w errdisable detect

DUT1# show errdisable detect

<table>
<thead>
<tr>
<th>ErrDisable Reason</th>
<th>Detection status</th>
</tr>
</thead>
<tbody>
<tr>
<td>bpduckguard</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
### 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

<table>
<thead>
<tr>
<th>ErrDisable Reason</th>
<th>Timer Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>bpdu-loop</td>
<td>Disabled</td>
</tr>
<tr>
<td>link-monitor-failure</td>
<td>Disabled</td>
</tr>
<tr>
<td>oam-remote-failure</td>
<td>Disabled</td>
</tr>
<tr>
<td>port-security</td>
<td>Disabled</td>
</tr>
<tr>
<td>link-flap</td>
<td>Disabled</td>
</tr>
<tr>
<td>udld</td>
<td>Disabled</td>
</tr>
<tr>
<td>fdb-loop</td>
<td>Disabled</td>
</tr>
<tr>
<td>loopback-detection</td>
<td>Disabled</td>
</tr>
<tr>
<td>reload-delay</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Timer interval: 300 seconds
```

**Related Commands**

errdisable recovery interval

errdisable recovery reason

#### 3.2.9 show errdisable flap

**Command Purpose**

Use this command to display error disable link flap parameters.
**Command Syntax**

show errdisable flap

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

This example shows how to display the flap configuration:

```
Switch# show errdisable flap
ErrDisable Reason      Flaps     Time (sec)
-------------------------------------------
link-flap              10         10
```

**Related Commands**

errdisable flap

---

**3.2.10 show errdisable fdb-loop**

**Command Purpose**

Use this command to display error disable fdb-loop parameters.

**Command Syntax**

show errdisable fdb-loop

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

When mac address migrates from one port to another port for 10 times in one minute, this mac address is considered as flapping and switch would print a flapping log for users. The log would be printed every 10 minutes.

**Examples**

This example shows how to display the fdb-loop configuration:

```
Switch# show errdisable fdb-loop
Errdisable FDB loop information
-------------------------------
Exclude VLAN-list : N/A
Detecting count   : 10
Detecting period  : 60s
Printing log period: 600s
```

**Related Commands**
3.2.11 errdisable fdb-loop trust

Command Purpose

Use this command to set trust mode on interface, and this interface would not be set error disable by fdb-loop detection.

Use the no form of this command to disable the error disable feature.

Command Syntax

errdisable fdb-loop trust

no errdisable fdb-loop trust

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

This example shows how to set trust mode on interface for fdb flap:

DUT1(config)# interface eth-0-1
DUT1(config-if)# errdisable fdb-loop trust

This example shows how to unset trust mode on interface for fdb flap:

DUT1(config)# interface eth-0-1
DUT1(config-if)# no errdisable fdb-loop trust

Related Commands

3.3 MAC Address Table Commands

3.3.1 mac-address-table ageing-time

Command Purpose

Use the mac-address-table ageing-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 ageing time applies to all VLANs.

Command Syntax

MAC_ADDRess-table ageing-time SECONDS

no MAC_ADDRess-table ageing-time

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>Aging time.</td>
<td>0, 10-1000000, 0 means that MAC aging function does not work, unit: second</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

The default is 300 seconds
Usage

If packets are not received continuously, user can increase the aging time to make the system recording the dynamic entries for a longer time. Increasing the time can reduce the possibility of flooding when the hosts send again.

Examples

This example shows how to set the aging time to 200 seconds for all VLANs:

```
Switch# configure terminal
Switch(config)# mac-address-table ageing-time 200
```

Related Commands

show mac address-table ageing-time

3.3.2 mac-address-table hardware-learning

Command Purpose

Use the mac-address-table hardware-learning enable global configuration command on the switch to study FDB without software. Use the no form of this command to return to the default setting.

Command Syntax

MAC_ADDRess-table hardware-learning enable
no MAC_ADDRess-table hardware-learning enable

Command Mode

Global Configuration

Default

Disable

Usage

Hardware learning is faster than software learning.

Examples

This example shows how to enable hardware learning:

```
Switch# configure terminal
Switch(config)# mac-address-table hardware-learning enable
```

Related Commands

None

3.3.3 mac-address-table forward

Command Purpose

Use the mac-address-table forward global configuration command on the switch to add static addresses to the MAC address table. Use the no form of this command to remove static entries from the table.

Command Syntax

MAC_ADDRess-table MAC_ADDR forward ( IFNAME | eps EPS_ID | remote-vtep REMOTE_VTEP_ID | smart-link SMART_LINK_ID ) vlan VLAN_ID

no MAC_ADDRess-table MAC_ADDR forward ( IFNAME | eps EPS_ID | remote-vtep REMOTE_VTEP_ID | smart-link SMART_LINK_ID ) vlan VLAN_ID
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC_ADDR</td>
<td>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</td>
<td>Mac address in HHHH.HHHH.HHHH format</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Interface to which the received packet is forwarded.</td>
<td>Valid interfaces include physical ports and link aggregation ports</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>Specify the VLAN for which the packet with the specified MAC address is received.</td>
<td>1-4094</td>
</tr>
<tr>
<td>EPS_ID</td>
<td>EPS protection group.</td>
<td>1-2048</td>
</tr>
<tr>
<td>REMOTE_VTEP_ID</td>
<td>Remote VTEP</td>
<td>1-65535</td>
</tr>
<tr>
<td>SMART_LINK_ID</td>
<td>Smart-Link Group</td>
<td>1-16</td>
</tr>
</tbody>
</table>

### Command Mode

Global Configuration

### Default

None

### Usage

The static address entries which are added by this command are not aged.

### Examples

This example shows how to add the static address c2f3220a12f4 to the MAC address table When a packet is received in VLAN 4 with this MAC address as its destination, the packet is forwarded to the specified interface:

```
Switch# configure terminal
Switch(config)# mac-address-table c2f3.220a.12f4 forward eth-0-1 vlan 4
```

### Related Commands

- show mac address-table

### 3.3.4 mac-address-table discard

#### Command Purpose

Use the mac-address-table discard global configuration command on the switch to enable unicast MAC address filtering and to configure the switch to drop traffic with a specific source or destination MAC address. Use the `no` form of this command to return to the default setting.

#### Command Syntax

```
MAC_ADDResstable MAC_ADDR discard
no MAC_ADDResstable MAC_ADDR discard
```
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC_ADDR</td>
<td>Source or Destination MAC address (unicast) to add to the address filtering table</td>
<td>-</td>
</tr>
</tbody>
</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 c2f3.220a.12f4. When a packet is received with this MAC address as its source or destination, the packet is dropped:

```
Switch# configure terminal
Switch(config)# mac-address-table c2f3.220a.12f4 discard
```

### Related Commands

mac-address-table forward

### 3.3.5 clear mac address-table

**Command Purpose**

Use the clear mac address-table privileged EXEC command on the switch to delete all dynamic(or static, or multicast) addresses, or all dynamic(or static, or multicast) addresses on a particular interface, or all dynamic(or static, or multicast) addresses on a particular VLAN from the MAC address table.

**Command Syntax**

```
clear mac address-table ( static | dynamic | multicast ) ( address MAC_ADDR | interface IFNAME | vlan VLAN_ID )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dynamic</td>
<td>Delete the dynamic MAC address</td>
<td>-</td>
</tr>
<tr>
<td>static</td>
<td>Delete the static MAC address</td>
<td>-</td>
</tr>
<tr>
<td>multicast</td>
<td>Delete the multicast MAC address</td>
<td>-</td>
</tr>
<tr>
<td>address MAC_ADDR</td>
<td>Delete the specified MAC address</td>
<td>Mac address in HHHH.HHHH.HHHH format</td>
</tr>
<tr>
<td>interface IFNAME</td>
<td>Delete all MAC addresses on the specified physical port or link aggregation port</td>
<td>Support physical/aggregation ports</td>
</tr>
<tr>
<td>vlan VLAN_ID</td>
<td>Delete all MAC addresses for the specified VLAN</td>
<td>1-4094</td>
</tr>
</tbody>
</table>
Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to remove a specific MAC address from the dynamic address table:

Switch# clear mac address-table dynamic address 0008.0070.0007

Related Commands
show mac address-table

3.3.6 port-bridge

Command Purpose
Use this command to support to forward packets with the src-mac and dset-mac learned by the same port.

Command Syntax
switchport port-bridge enable
no switchport port-bridge enable

Command Mode
Interface Configuration

Default
None

Usage
None

Examples
This example shows how to enable port-bridge function:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport port-bridge enable

Related Commands

3.3.7 show mac address-table ageing-time

Command Purpose
Use the show mac address-table ageing-time privileged EXEC command to display the aging time of all address table instances on all VLANs.

Command Syntax
show mac address-table ageing-time

Command Mode
Privileged EXEC
Default
None

Usage
None

Examples
This is an example of output from the show mac address-table ageing-time command:

Switch# show mac address-table ageing-time
MAC address table ageing time is 300 seconds

Related Commands
mac-address-table ageing-time

3.3.8 show mac address-table

Command Purpose
Use the show mac address-table privileged EXEC command to display a specific MAC address table static and dynamic entry or the MAC address table static and dynamic entries on a specific interface or VLAN.

Command Syntax
show mac address-table ( dynamic | static | multicast ) ( address MAC_ADDR | interface IFNAME | vlan VLAN_ID )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dynamic</td>
<td>Display the dynamic MAC address</td>
<td>-</td>
</tr>
<tr>
<td>static</td>
<td>Display the static MAC address</td>
<td>-</td>
</tr>
<tr>
<td>multicast</td>
<td>Display the multicast MAC address</td>
<td>-</td>
</tr>
<tr>
<td>address MAC_ADDR</td>
<td>Display the specified MAC address</td>
<td>Mac address in HHHH.HHHH.HHHH format</td>
</tr>
<tr>
<td>interface IFNAME</td>
<td>Display all MAC addresses on the specified physical port or link aggregation port</td>
<td>Support physical/aggregation ports</td>
</tr>
<tr>
<td>vlan VLAN_ID</td>
<td>Display all MAC addresses for the specified VLAN.</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Mac Address Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>(*) - Security Entry  (M) - MLAG Entry  (MO) - MLAG Output Entry  (MI) - MLAG Input Entry</td>
</tr>
<tr>
<td>Vlan</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>1</td>
</tr>
</tbody>
</table>

Related Commands

mac-address-table

3.3.9 show mac address-table hardware

Command Purpose

Use the show mac address-table hardware privileged EXEC command to display a specific MAC address table static and dynamic entry or the MAC address table static and dynamic entries on a specific interface or VLAN in hardware.

Command Syntax

show mac address-table hardware { dynamic | static } { ( address MAC_ADDR | interface IFNAME | vlan VLAN_ID ) }

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dynamic</td>
<td>Display the dynamic MAC address</td>
<td>-</td>
</tr>
<tr>
<td>static</td>
<td>Display the static MAC address</td>
<td>-</td>
</tr>
<tr>
<td>address MAC_ADDR</td>
<td>Display the specified MAC address</td>
<td>Mac address in HHHH.HHHH.HHHH format</td>
</tr>
<tr>
<td>interface IFNAME</td>
<td>Display all MAC addresses on the specified physical port or link aggregation port</td>
<td>Support physical/aggregation ports</td>
</tr>
<tr>
<td>vlan VLAN_ID</td>
<td>Display all MAC addresses for the specified VLAN.</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Mac Address Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>(*) - Security Entry  (M) - MLAG Entry</td>
</tr>
</tbody>
</table>

www.fs.com
### Related Commands

- `mac-address-table`

#### 3.3.10 show mac address-table count

**Command Purpose**

Use the `show mac address-table count` privileged EXEC command to display the number of addresses present in all VLANs.

**Command Syntax**

`show mac address-table count`

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

This is an example of output from the `show mac address-table count` command:

```
Switch# show mac address-table count

Dynamic Address Count : 1  (Security: 0)
Static Address Count  : 1  (Security: 0)
Total Mac Addresses   : 2  (Security: 0)
```

**Related Commands**

- `show mac address-table`

#### 3.3.11 show mac address-table hardware count

**Command Purpose**

Use the `show mac address-table hardware count` privileged EXEC command to display the number of addresses present in all VLANs in hardware.

**Command Syntax**

`show mac address-table hardware count`

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None
Examples

This is an example of output from the show mac address-table hardware count command:

```
Switch# show mac address-table hardware count
MAC address count in hardware table:
(Include MAC security entry)
-------------------------------------------
Dynamic Address Count : 0
Static Address Count  : 0
Total Mac Addresses   : 0
```

Related Commands

```
show mac address-table hardware
```

3.3.12 show mac address-table add-fdb-fail

Command Purpose

Use the show mac address-table add-fdb-fail privileged EXEC command to display all failed static FDB entries when adding FDB table in chip for hash conflict.

Command Syntax

```
show mac address-table add-fdb-fail
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This is an example of output from the show mac address-table add-fdb-fail command:

```
Switch# show mac address-table add-fdb-fail

Vlan  | Mac Address    | Type   | Ports
-----|----------------|--------|-------
 1    | 0000.0000.0001 | static | eth-0-1
 1    | 0000.0000.0002 | static | eth-0-2
```

Related Commands

```
show mac address-table
```

3.3.13 show mac-filter address-table

Command Purpose

Use the show mac-filter address-table privileged EXEC command to display the number of filter addresses present in all VLANs.

Command Syntax

```
show mac-filter address-table
```

Command Mode

Privileged EXEC
Default
None

Usage
None

Examples
This is an example of output from the show mac-filter address-table command:

```
Switch# show mac-filter address-table

MAC Filter Address Table
----------------------------------
Current count : 0
Max count : 128
Left count : 128
Filter address list :
----------------------------------
```

Related Commands
show mac address-table

3.3.14 show resource mac-filter

Command Purpose
Use this command to display the resource statistic used by mac-filter.

Command Syntax
show resource mac-filter

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following is sample output from the show resource mac-filter command:

```
Switch# show resource mac-filter

MAC-FILTER Resource Used Capability
==================================
Blackhole MAC Addresses 0 128
```

Related Commands
show resource static-fdb

3.3.15 show resource static-fdb

Command Purpose
Use this command to display the resource statistic used by static FDB.

Command Syntax
show resource static-fdb
Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following is sample output from the show resource static-fdb command:

```
Switch# show resource static-fdb

STATIC-FDB
Resource Used Capability
-----------------------
Static FDB 0 1024
```

Related Commands
show resource mac-filter

3.4 VLAN Commands

3.4.1 vlan database

Command Purpose
Use this command to enter VLAN configure mode.

Command Syntax

```
vlan database
```

Command Mode
Global Configuration

Default
None

Usage

When you try to create or remove VLAN, you must use this command to enter VLAN configure mode first. To exit VLAN configure mode, use exit command.

Examples

This example shows how to enter VLAN configure mode:

```
Switch# 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
<tr>
<td>NAME</td>
<td>the name for specific vlan,</td>
<td>A string with no more than 31 characters</td>
</tr>
<tr>
<td>enable</td>
<td>set the operational stateof the VLAN to enable, and it is enabled by default</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>set the operational state of the VLAN to disable</td>
<td>-</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
<tr>
<td>SLOT_ID</td>
<td>The slot id of the port</td>
<td>-</td>
</tr>
<tr>
<td>PORT_ID</td>
<td>The port id of the port</td>
<td>-</td>
</tr>
</tbody>
</table>

**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**

```plaintext
vlan VLAN_LIST
```

```plaintext
no vlan VLAN_LIST
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_LIST</td>
<td>vlan list</td>
<td>vlan list connected with <code>-</code> and <code>,</code> for example, &quot;1-10,15,20,30-40&quot;</td>
</tr>
</tbody>
</table>

**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 cannot 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Name</th>
<th>State</th>
<th>STP ID</th>
<th>Member ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>VLAN0011</td>
<td>ACTIVE</td>
<td>0</td>
<td>eth-0:3(u) eth-0-4(t)</td>
</tr>
</tbody>
</table>

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:

```
Switch# show vlan all

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Name</th>
<th>State</th>
<th>STP ID</th>
<th>Member ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>default</td>
<td>ACTIVE</td>
<td>0</td>
<td>eth-0-1(u) eth-0-2(u)</td>
</tr>
<tr>
<td>11</td>
<td>VLAN0011</td>
<td>ACTIVE</td>
<td>0</td>
<td>eth-0-3(u) eth-0-4(t)</td>
</tr>
</tbody>
</table>
```

**Related Commands**
show 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

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Name</th>
<th>State</th>
<th>STP ID</th>
<th>Member ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>default</td>
<td>ACTIVE</td>
<td>0</td>
<td>eth-0-1(u) eth-0-2(u)</td>
</tr>
<tr>
<td>10</td>
<td>VLAN0010</td>
<td>ACTIVE</td>
<td>0</td>
<td>eth-0-3(u)</td>
</tr>
</tbody>
</table>
```

**Related Commands**
show 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 | ]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support aggregation and physical ports</td>
</tr>
</tbody>
</table>

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 specified vlan
Command Syntax

switchport access allowed vlan ( add | remove ) VLAN_ID_LIST

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>add the port to the specified vlan</td>
<td>-</td>
</tr>
<tr>
<td>remove</td>
<td>remove the port from the specified vlan</td>
<td>-</td>
</tr>
</tbody>
</table>

| 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan id</td>
<td>2-4094</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

All ports are default in vlan 1
Usage

Usage

Used the switchport mode access command to switch the port to access mode before use this command.

Examples

This example shows how to add the access port to vlan11:

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

This example shows how to revert the port to vlan1:

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

Related Commands

switchport mode access

3.4.11 switchport mode access

Command Purpose

Use this command to switch port to access mode.

Command Syntax

switchport mode access

Command Mode

Interface Configuration

Default

None

Usage

Access mode used to connect terminal, e.g:PC. The FDB on the port will be cleared when switch the port mode.

Examples

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

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

Related Commands

switchport mode trunk

3.4.12 switchport mode trunk

Command Purpose

Use this command to switch port to trunk mode.

Command Syntax

switchport mode trunk

Command Mode

Interface Configuration
Default
None

Usage
Trunk mode used to connect switch device or terminal. The FDB on the port will be cleared when switch the port mode.

Examples
This example shows how to set the port to trunk mode:

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

Related Commands
switchport mode access

3.4.13 switchport trunk allowed

Command Purpose
Use this command to allow or remove the trunk port to the specified

Command Syntax
```
switchport trunk allowed vlan ( add VLAN_ID_LIST | remove VLAN_ID_LIST | all | none )
```

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
```

**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 untagged 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID_LIST</td>
<td>vlan list</td>
<td>Connected with <code>-</code> and `,” for example,”1-10,15,20,30-40”</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

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

3.4.17 vlan statistics enable

Command Purpose
Use this command to enable the statistics of VLAN.
To disable the statistics, use the no form of this command.

Command Syntax
vlan VLAN_ID statistics enable
no vlan VLAN_ID statistics enable

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>An existing Vlan id</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode
VLAN Configuration

Default
inactive

Usage
none

Examples
This example shows how to enable the statistics of vlan 2:

Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2 statistics enable

This example shows how to disable the statistics of vlan 2:

Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# no vlan 2 statistics enable

Related Commands
vlan statistics interval
clear vlan statistics
show vlan vlan statistics
3.4.18 vlan statistics interval

Command Purpose
Use this command to set sample interval.
To restore to default value, use the no form of this command.

Command Syntax

<table>
<thead>
<tr>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan statistics interval VALUE</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VALUE</td>
<td>Sample interval</td>
<td>5-600, unit: second</td>
</tr>
</tbody>
</table>

Command Mode
VLAN Configuration

Default
10s

Usage
none

Examples
This example shows how to set sample interval:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan statistics interval 20
```

Related Commands

- vlan statistics enable
- clear vlan statistics
- show vlan vlan statistics

3.4.19 clear vlan statistics

Command Purpose
Use this command to clear statistics information.

Command Syntax

<table>
<thead>
<tr>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear wlan VLAN_ID statistics</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>An existing Vlan id</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
none

Usage
none
Examples
This example shows how to clear vlan statistics:
Switch# clear vlan 2 statistics

Related Commands
vlan statistics enable
vlan statistics interval
show vlan vlan statistics

3.4.20 show vlan statistics

Command Purpose
Use this command to show statistics information.

Command Syntax
show vlan VLAN_ID statistics

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>An existing Vlan id</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
none

Usage
none

Examples
This example shows how to show vlan statistics:
Switch# show vlan 2 statistics
VLAN: 2

<table>
<thead>
<tr>
<th>Item</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound:</td>
<td>3654365</td>
</tr>
<tr>
<td>Outbound:</td>
<td>3654365</td>
</tr>
</tbody>
</table>

Related Commands
vlan statistics enable
vlan statistics interval

3.4.21 show resource vlan-stats

Command Purpose
Use this command to show the resource statistic used by vlan statistics.

Command Syntax
show resource vlan-stats

Command Mode
Privileged EXEC
Examples

This example shows how to show resource used by vlan statistics:

Switch# show resource vlan-stats

<table>
<thead>
<tr>
<th>VLAN-STATS</th>
<th>Used</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applied VLAN Stats Entry</td>
<td>1</td>
<td>128</td>
</tr>
</tbody>
</table>

Related Commands

vlan statistics enable

3.5 Voice VLAN Commands

3.5.1 voice vlan

Command Purpose

Use this command to specific VLAN as VOICE VLAN.

Command Syntax

voice vlan VLAN_ID

no voice vlan

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan id</td>
<td>2-4094</td>
</tr>
</tbody>
</table>

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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>COS</td>
<td>cos value</td>
<td>0-7</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC</td>
<td>Source MAC address (unicast or multicast) to add to the address table</td>
<td>MAC Address in HHHH.HHHH.HHHH format</td>
</tr>
<tr>
<td>MASK</td>
<td>The MASK for the Source MAC</td>
<td>MAC Mask in HHHH.HHHH.HHHH format</td>
</tr>
<tr>
<td>LINE</td>
<td>The description for this OUI</td>
<td>Up to 63 characters</td>
</tr>
</tbody>
</table>

**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 VOICE VLAN.

Command Syntax
show voice vlan state

Command Mode
Privileged EXEC

Default
None

Usage
This command is used to show the current status of VOICE VLAN.

Examples
This example shows how to show the current status of VOICE 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_NUMBER</td>
<td>Channel group number</td>
<td>1-55</td>
</tr>
<tr>
<td>active</td>
<td>Enable initiation of LACP negotiation on a port</td>
<td>-</td>
</tr>
<tr>
<td>passive</td>
<td>Disable initiation of LACP negotiation on a port</td>
<td>-</td>
</tr>
</tbody>
</table>
### 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_NUMBER</td>
<td>Channel group number</td>
<td>1-55</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRIORITY</td>
<td>LACP port priority</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>short</td>
<td>Set LACP short timeout</td>
<td>-</td>
</tr>
<tr>
<td>long</td>
<td>Set LACP long timeout</td>
<td>-</td>
</tr>
</tbody>
</table>
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(config-if)# lacp timeout short
```

This example shows how to return to the default setting:

```
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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRIORITY</td>
<td>LACP system priority</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

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(config-if)# lacp system-priority 100
```

This example shows how to return to the default setting:

```
Switch(config-if)# no lacp system-priority
```

Related Commands
None
3.6.6 port-channel load-balance hash-field-select

**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-ippsa | inner-ip-protocol | inner-macda | inner-macsa | inner-sourceport | inner-destport | src-interface }
```

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>macda</td>
<td>Load balance by destination MAC address</td>
<td>-</td>
</tr>
<tr>
<td>macsa</td>
<td>Load balance by source MAC address</td>
<td>-</td>
</tr>
<tr>
<td>ipda</td>
<td>Load balance by destination IP address</td>
<td>-</td>
</tr>
<tr>
<td>ipsa</td>
<td>Load balance by source IP address</td>
<td>-</td>
</tr>
<tr>
<td>srcport</td>
<td>Load balance by source port</td>
<td>-</td>
</tr>
<tr>
<td>dstport</td>
<td>Load balance by destination port</td>
<td>-</td>
</tr>
<tr>
<td>ip-protocol</td>
<td>Load balance by ip-protocol</td>
<td>-</td>
</tr>
<tr>
<td>nvgre-vsid</td>
<td>Vsid of nvgre</td>
<td>-</td>
</tr>
<tr>
<td>vxlan-vni</td>
<td>Vni of vxlan</td>
<td>-</td>
</tr>
<tr>
<td>inner-destport</td>
<td>Inner Destination port based load balancing</td>
<td>-</td>
</tr>
<tr>
<td>inner-ip-protocol</td>
<td>Inner Ip-protocol based load balancing</td>
<td>-</td>
</tr>
<tr>
<td>inner-ipda</td>
<td>Inner Destination IP address based load balancing</td>
<td>-</td>
</tr>
<tr>
<td>inner-ipsa</td>
<td>Inner Source IP address based load balancing</td>
<td>-</td>
</tr>
<tr>
<td>inner-macda</td>
<td>Inner Destination MAC address based load balancing</td>
<td>-</td>
</tr>
<tr>
<td>inner-macsa</td>
<td>Inner Source MAC address based load balancing</td>
<td>-</td>
</tr>
<tr>
<td>inner-sourceport</td>
<td>Inner Source port based load balancing</td>
<td>-</td>
</tr>
<tr>
<td>src-interface</td>
<td>Load balance by source interface the packet input</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

`ipda ipsa dstport srcport ip-protocol`

**Usage**

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

**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 hash-field-select macsa

Related Commands
None

3.6.7 port-channel load-balance hash-arithmetic

Command Purpose
Use this command to configure the load balance hash algorithm 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-arithmetic (xor | crc )

no port-channel load-balance hash-arithmetic

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>xor</td>
<td>Use algorithm of exclusive or to compute hash value</td>
<td>-</td>
</tr>
<tr>
<td>crc</td>
<td>Use algorithm of crc to compute hash value</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
Xor

Usage
None

Examples
This example shows how to configure the load balance hash algorithm for Link Aggregation Control Protocol (LACP), use crc:

Switch# configure terminal
Switch(config)# port-channel load-balance hash-arithmetic crc

This example shows how to configure the load balance hash algorithm for Link Aggregation Control Protocol (LACP), use xor:

Switch# configure terminal
Switch(config)# port-channel load-balance hash-arithmetic xor

Related Commands
None

3.6.8 port-channel channel-group-number load-balance-mode dynamic

Command Purpose
Use this command to enable dynamic load balance for the Link Aggregation Group (both static and dynamic aggregator). Use the no form of this command to return to the default setting.

Command Syntax
port-channel GROUP_NUMBER load-balance-mode dynamic

no port-channel channel-group-number load-balance-mode

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_NUMBER</td>
<td>Channel group number</td>
<td>1-55</td>
</tr>
</tbody>
</table>
Command Mode
Global Configuration

Default
None

Usage
Before enable or disable the load-balance mode, the Link Aggregation Group should not be create.

Examples
This example shows how to enable dynamic load balance for agg1:

Switch# configure terminal
Switch(config)# port-channel 1 load-balance-mode dynamic

Related Commands
None

3.6.9 port-channel channel-group-number load-balance-mode round-robin

Command Purpose
Use this command to enable round-robin load balance for the Link Aggregation Group (both static and dynamic aggregator). Use the no form of this command to return to the default setting.

Command Syntax
port-channel GROUP_NUMBER load-balance-mode round-robin

no port-channel GROUP_NUMBER load-balance-mode

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_NUMBER</td>
<td>Channel group number</td>
<td>1-55</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
Before enable or disable the load-balance mode, the Link Aggregation Group should not be create.

Examples
This example shows how to enable round-robin load balance for agg1:

Switch# configure terminal
Switch(config)# port-channel 1 load-balance-mode round-robin

Related Commands
None

3.6.10 port-channel channel-group-number self-healing

Command Purpose
Use this command to enable self-healing for the Link Aggregation Group (both static and dynamic aggregator). Use the no form of this command to return to the default setting.
Command Syntax

port-channel GROUP_NUMBER self-healing

no port-channel GROUP_NUMBER self-healing

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_NUMBER</td>
<td>Channel group number</td>
<td>1-55</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

Before enable or disable the self-healing, the Link Aggregation Group should not be create.

Examples

This example shows how to enable self-healing for agg1:

Switch# configure terminal
Switch(config)# port-channel 1 self-healing

Related Commands

None

3.6.11 port-channel channel-group-number static

Command Purpose

Use this command to enable static load balance for the Link Aggregation Group (both static and dynamic aggregator). Use the no form of this command to return to the default setting.

Command Syntax

port-channel GROUP_NUMBER load-balance-mode static

no port-channel channel-group-number load-balance-mode

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_NUMBER</td>
<td>Channel group number</td>
<td>1-55</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

Before enable or disable the load-balance mode, the Link Aggregation Group should not be create.

Examples

This example shows how to enable static load balance for agg1:

Switch# configure terminal
Switch(config)# port-channel 1 load-balance-mode static
3.6.12 port-channel channel-group-number lACP-mode dynamic

Command Purpose
Use this command to enable dynamic lACP for the Link Aggregation Group (only dynamic aggregator). Use the no form of this command to unset the setting.

Command Syntax

```
port-channel GROUP_NUMBER lACP-mode dynamic
no port-channel GROUP_NUMBER lACP-mode
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_NUMBER</td>
<td>Channel group number</td>
<td>1-55</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
Before enable or disable the dynamic lACP mode, the Link Aggregation Group should not be create.

Examples
This example shows how to enable dynamic lACP-mode for agg1:

```
NoneSwitch# configure terminal
Switch(config)# port-channel 1 lACP-mode dynamic
```

Related Commands

3.6.13 port-channel group-mode

Command Purpose
Use this command to switch the Link Aggregation Group mode. Use the no form of this command to return to the default group mode(56).

Command Syntax

```
port-channel group-mode (8 | 16 | 32 | 56 )
no port-channel group-mode
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Group mode 8, the group range is 1~7</td>
<td>8</td>
</tr>
<tr>
<td>16</td>
<td>Group mode 16, the group range is 1~15</td>
<td>16</td>
</tr>
<tr>
<td>32</td>
<td>Group mode 32, the group range is 1~31</td>
<td>32</td>
</tr>
<tr>
<td>56</td>
<td>Group mode 32, the group range is 1~55</td>
<td>56</td>
</tr>
</tbody>
</table>
**Command Mode**

Global Configuration

**Default**

56

**Usage**

The linkagg group-mode you specified will not take effect until you save configuration and reboot

**Examples**

This example shows how to switch to group mode 32:

```
Switch# configure terminal
Switch(config)# port-channel group-mode 32
```

**Related Commands**

None

3.6.14 show channel-group summary

**Command Purpose**

Use this command to display a summary of all of the channel groups, or a specified channel group.

**Command Syntax**

```
show channel-group { channel-group-number | } summary
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>channel-group-number</td>
<td>Channel group number</td>
<td>1-55</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

This example shows how to display a summary of all of the channel groups:

```
Switch# show channel-group summary

port-channel load-balance hash-arithmetic: xor
port-channel load-balance hash-field-select: ipsa ipd a srcport dstport ip-protocol
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

Mode:     SLB  - Static load balance
          DLB  - Dynamic load balance
          SHLB - Self-healing load balance
          RR   - Round robin load balance

Aggregator Name | Mode | Protocol | Ports
----------------|------|----------|--------
agg4(SD)        | SLB  | Static   | eth-0-10(D)
```

www.fs.com
3.6.15 show channel-group detail

Command Purpose
Use this command to display detailed information of all of the channel groups, or a specified channel group.

Command Syntax
show channel-group (GROUP_NUMBER | ) detail

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_NUMBER</td>
<td>Channel group number</td>
<td>1-55</td>
</tr>
</tbody>
</table>

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
3.6.16 show lacp internal

Command Purpose
Use this command to display internal information of all of the channel groups, or a specified channel group.

Command Syntax
show lacp (GROUP_NUMBER | ) internal

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_NUMBER</td>
<td>Channel group number</td>
<td>1-55</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>LACP port Admin Priority</th>
<th>Oper Key</th>
<th>Port Number</th>
<th>Port State</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-0-9</td>
<td>SA bndl</td>
<td>32768</td>
<td>1</td>
<td>1</td>
<td>0x9</td>
<td>0x3d</td>
</tr>
</tbody>
</table>

Related Commands
None

3.6.17 show lacp internal detail

Command Purpose
Use this command to display detailed internal information of all of the channel groups, or a specified channel group.

Command Syntax
show lacp (GROUP_NUMBER | ) internal detail

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_NUMBER</td>
<td>Channel group number</td>
<td>1-55</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Port</th>
<th>Actor System ID</th>
<th>Actor Port Number</th>
<th>Actor Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-0-9</td>
<td>32768, e0ef.1a32.7e00</td>
<td>0x9</td>
<td>SA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LACP Actor</th>
<th>Actor Port Priority</th>
<th>Actor Oper Key</th>
<th>Actor Port State</th>
</tr>
</thead>
<tbody>
<tr>
<td>32768</td>
<td>1</td>
<td>0x4d</td>
<td></td>
</tr>
</tbody>
</table>

Port State Flags Decode:
- Activity: Active
- Timeout: Long
- Aggregation: Yes
- Synchronization: Yes

Collecting: No
Distributing: No
Defaulted: Yes
Expired: No

Related Commands

None

3.6.18 show lACP neighbor

Command Purpose

Use this command to display neighbor information of all of the channel groups, or a specified channel group.

Command Syntax

```
show lACP { GROUP_NUMBER | } neighbor
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_NUMBER</td>
<td>Channel group number</td>
<td>1-55</td>
</tr>
</tbody>
</table>

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:
### 3.6.19 show lACP neighbor detail

**Command Purpose**

Use this command to display detailed neighbor information of all of the channel groups, or a specified channel group.

**Command Syntax**

`show lACP (GROUP_NUMBER | ) neighbor detail`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_NUMBER</td>
<td>Channel group number</td>
<td>1-55</td>
</tr>
</tbody>
</table>

**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 LACPDU's  
- F - Device is requesting Fast LACPDU's  
- A - Device is in Active mode  
- P - Device is in Passive mode  

Channel group 1 neighbors  
Partner's information:  
```
<table>
<thead>
<tr>
<th>Port</th>
<th>System ID</th>
<th>Port Number</th>
<th>Flags</th>
<th>LACP Port Priority</th>
<th>Oper Key</th>
<th>Port State</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-0-9</td>
<td>32768,0000.0000.0000</td>
<td>0x0</td>
<td>SP</td>
<td>0</td>
<td>0</td>
<td>0x44</td>
</tr>
</tbody>
</table>
```

Port State Flags Decode:  
- Activity: Passive  
- Timeout: Long  
- Aggregation: Yes  
- Synchronization: No  
- Collecting: No  
- Distributing: No  
- Defaulted: Yes  
- Expired: No

**Related Commands**

None
3.6.20 show channel-group port

Command Purpose

Use this command to display details of the LACP port of all of the channel groups, or a specified channel group, or a specified port.

Command Syntax

show channel-group port ( IFNAME | )
show channel-group GROUP_NUMBER port

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical ports</td>
</tr>
<tr>
<td>GROUP_NUMBER</td>
<td>Channel group number</td>
<td>1-55</td>
</tr>
</tbody>
</table>

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  A - Device is in active mode
             F - Device is sending fast LACPDUs  P - Device is in passive mode

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

      Partner's information:
      Port   Flags LACP port Priority Dev ID Oper Key Port Number Port 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:

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>Priority</th>
<th>Admin Key</th>
<th>Oper Key</th>
<th>Port Number</th>
<th>Port State</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-0-9</td>
<td>SA</td>
<td>indep</td>
<td>32768</td>
<td>1</td>
<td>1</td>
<td>9</td>
<td>0x4d</td>
</tr>
</tbody>
</table>

Partner's information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>LACP port</th>
<th>Priority</th>
<th>Dev ID</th>
<th>Oper</th>
<th>Port Number</th>
<th>Port State</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-0-9</td>
<td>SP</td>
<td>0</td>
<td>0000.0000.0000</td>
<td>0</td>
<td>0</td>
<td>0x44</td>
<td></td>
</tr>
</tbody>
</table>

**Related Commands**

None

### 3.6.21 show lacp counters

**Command Purpose**

Use this command to display the packet traffic on all of the channel groups, or a specified channel group.

**Command Syntax**

`show lacp [GROUP_NUMBER] counters`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_NUMBER</td>
<td>Channel group number</td>
<td>1-55</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Port</th>
<th>LACPDU</th>
<th>Pkts err</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sent</td>
<td>Recv</td>
</tr>
<tr>
<td></td>
<td>Sent</td>
<td>Recv</td>
</tr>
</tbody>
</table>

Channel-group agg1

eth-0-9   46   38    0    0
```

**Related Commands**

None
### 3.6.22 show lACP sys-id

**Command Purpose**

Use this command to display the LACP system ID.

**Command Syntax**

```
show lACP sys-id
```

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

This example shows how to display the LACP system ID:

```
Switch# show lACP sys-id
System ID: 32768,4600.0987.6c01
```

**Related Commands**

None

### 3.6.23 clear lACP counters

**Command Purpose**

Use this command to clear all counters of all of the channel groups, or a specified channel group.

**Command Syntax**

```
clear lACP (GROUP_NUMBER | ) counters
```

```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_NUMBER</td>
<td>Channel group number</td>
<td>1-55</td>
</tr>
</tbody>
</table>
```

**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

---

www.fs.com
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)
```

```
ovlan classifier activate
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_NUMBER</td>
<td>VLAN classifier group id</td>
<td>0-31, only group id 31 can be used for protocol</td>
</tr>
<tr>
<td>ip</td>
<td>Based on ip</td>
<td>-</td>
</tr>
<tr>
<td>mac</td>
<td>Based on MAC</td>
<td>-</td>
</tr>
<tr>
<td>protocol</td>
<td>Based on protocol</td>
<td>-</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_NUMBER</td>
<td>VLAN classifier group id</td>
<td>0-31, only group id 31 can be used for protocol</td>
</tr>
<tr>
<td>add</td>
<td>Add rule to vlan classifier group</td>
<td>-</td>
</tr>
<tr>
<td>delete</td>
<td>Delete rule to vlan classifier group</td>
<td>-</td>
</tr>
<tr>
<td>RULE</td>
<td>The id of rule</td>
<td>0-4095</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RULE</td>
<td>The id of vlan classifier rule</td>
<td>0-4095</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>The source of ipv4 address in packets</td>
<td>IPv4 address</td>
</tr>
<tr>
<td>IPV6_ADDR</td>
<td>The source of ipv6 address in packets</td>
<td>IPv6 address</td>
</tr>
<tr>
<td>MAC_ADDR</td>
<td>The source of mac address in packets</td>
<td>Mac address in HHHH.HHHH.HHHH format</td>
</tr>
<tr>
<td>protocol</td>
<td>Specify an ethernet protocol classification</td>
<td>-</td>
</tr>
<tr>
<td>arp</td>
<td>Specify ARP protocol</td>
<td>-</td>
</tr>
<tr>
<td>ip</td>
<td>Specify IP protocol</td>
<td>-</td>
</tr>
<tr>
<td>mpls</td>
<td>Specify MPLS protocol</td>
<td>-</td>
</tr>
<tr>
<td>mpls-mcast</td>
<td>Specify MPLS multicast protocol</td>
<td>-</td>
</tr>
<tr>
<td>pppoe</td>
<td>Specify PPPOE protocol</td>
<td>-</td>
</tr>
<tr>
<td>rarp</td>
<td>Specify RARP protocol</td>
<td>-</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>The vlan id to be assigned</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

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 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_ID</td>
<td>VLAN classifier group id</td>
<td>0-31, only group id 31 can be used for protocol</td>
</tr>
</tbody>
</table>

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

3.7.5 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_ID</td>
<td>VLAN classifier group id</td>
<td>0-31, only group id 31 can be used for protocol</td>
</tr>
</tbody>
</table>

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

3.7.6 show vlan classifier rule

Command Purpose
Use this command to show the information about vlan classifier rule.

Command Syntax
show vlan classifier rule (RULE )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RULE</td>
<td>The id of vlan classifier rule</td>
<td>0-4095</td>
</tr>
</tbody>
</table>

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

3.7.7 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

<table>
<thead>
<tr>
<th>VLAN-CLASS</th>
<th>Resource</th>
<th>Used</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Based VLAN Classification</td>
<td>0</td>
<td>512</td>
<td></td>
</tr>
<tr>
<td>IPv4 Based VLAN Classification</td>
<td>0</td>
<td>512</td>
<td></td>
</tr>
</tbody>
</table>
```

Related Commands

None

3.8 VLAN Mapping Commands

3.8.1 ethernet evc

Command Purpose

Use this command to add or delete EVC table.

Command Syntax

```
ethernet evc WORD

no ethernet evc WORD
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>EVC name</td>
<td>Up to 16 characters</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

None

Examples

Create ethernet evc evc_table:

```
Switch# configure terminal
Switch(config)# ethernet evc evc_table
Switch(config-evc)# dot1q mapped-vlan 10
```

Related Commands

show ethernet evc NAME

3.8.2 dot1q mapped-vlan

Command Purpose

Use this command to add evc entry to EVC table.

```
dot1q mapped-vlan VLAN_ID
```

Command Syntax

```
no dot1q mapped-vlan
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Mapped vlan id</td>
<td>1-4094</td>
</tr>
</tbody>
</table>
**Command Mode**

EVC Configuration

**Default**

None

**Usage**

None

**Examples**

Add EVC mapped-vlan entry, mapped vlan is 100:

Switch# configure terminal
Switch(config)# ethernet evc evc_table
Switch(config-evc)# dot1q mapped-vlan 100

**Related Commands**

show ethernet evc NAME

---

### 3.8.3 dot1q mapped-double-vlan

**Command Purpose**

Use this command to add evc entry with double vlans to EVC table.

**Command Syntax**

```
dot1q mapped-double-vlan INNER_VLAN_ID OUTER_VLAN_ID
```

```
no dot1q mapped-double-vlan
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INNER_VLAN_ID</td>
<td>Mapped inner vlan id</td>
<td>1-4094</td>
</tr>
<tr>
<td>OUTER_VLAN_ID</td>
<td>Mapped outer vlan id</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

**Command Mode**

EVC Configuration

**Default**

None

**Usage**

This command is only used for untagged packet

**Examples**

Add EVC mapped-vlan entry, mapped inner vlan is 100, mapped outer vlan is 10:

Switch# configure terminal
Switch(config)# ethernet evc evc_table
Switch(config-evc)# dot1q mapped-double-vlan 100 10

**Related Commands**

show ethernet evc NAME

---

### 3.8.4 vlan mapping table

**Command Purpose**

Use this command to add or delete vlan mapping table.
### Command Syntax

**vlan mapping table** WORD

no **vlan mapping table** WORD

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>The name of vlan mapping table</td>
<td>Up to 16 characters</td>
</tr>
</tbody>
</table>

#### Command Mode

**Global Configuration**

**Default**

None

**Usage**

None

#### Examples

Create vlan mapping table VMT:

```
Switch# configure terminal
Switch(config)# vlan mapping table VMT
Switch(config-vlan-mapping)#
```

**Related Commands**

show vlan mapping table WORD

### 3.8.5 raw vlan group

#### Command Purpose

Use this command to create raw VLAN group.

#### Command Syntax

```
raw vlan group GROUP_ID vlan VLAN_LIST
```

no raw vlan group GROUP_ID

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_ID</td>
<td>Raw vlan group id</td>
<td>1-64</td>
</tr>
<tr>
<td>VLAN_LIST</td>
<td>The VLAN ID list, example: 2-5,9-11</td>
<td>vlan list connected with ‘-’ and ‘,’ for example, “1-10,15,20,30-40”</td>
</tr>
</tbody>
</table>

#### Command Mode

**Global Configuration**

**Default**

None

**Usage**

None

#### Examples

Create raw VLAN group 1 and the VLAN list is from 10 to 20:

```
Switch# configure terminal
Switch(config)# raw vlan group 1 vlan 10-20
```
Related Commands
show vlan mapping table WORD

3.8.6 raw-vlan
Command Purpose
Use this command to add vlan mapping entry into vlan mapping table.

Command Syntax
raw-vlan (VLAN_ID | out-of-range | untagged | group GROUP_ID) evc WORD
no raw-vlan (VLAN_ID | out-of-range | untagged | group )
raw-vlan INNER_VLAN OUTER_VLAN egress-vlan (untagged | MAPPED_VLAN)
no raw-vlan INNER_VLAN OUTER_VLAN egress-vlan

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Raw vlan id, range from 1~4094,</td>
<td>vlan list connected with “,” and “,” for example,”1,10,15,20,30-40”</td>
</tr>
<tr>
<td>out-of-range</td>
<td>Vlan id isn’t specified</td>
<td>-</td>
</tr>
<tr>
<td>untagged</td>
<td>Untagged packet</td>
<td>-</td>
</tr>
<tr>
<td>group GROUP_ID</td>
<td>Raw VLAN group, the group will use less resource compare with VLAN range.</td>
<td>1-64</td>
</tr>
<tr>
<td>WORD</td>
<td>EVC name</td>
<td>Up to 16 characters</td>
</tr>
<tr>
<td>INNER_VLAN</td>
<td>Inner vlan id</td>
<td>1-4094</td>
</tr>
<tr>
<td>OUTER_VLAN</td>
<td>Outer vlan id</td>
<td>1-4094</td>
</tr>
<tr>
<td>MAPPED_VLAN</td>
<td>Mapped vlan id</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode
VLAN Mapping Configuration

Default
None

Usage
None

Examples
Add vlan mapping entry, raw vlan is from 10 to 20, mapped evc is evc_table:

Switch# configure terminal
Switch(config)# vlan mapping table VMT
Switch(config)# vlan mapping table VMT
Switch(config-vlan-mapping)# raw-vlan 10-20 evc evc_table

Related Commands
show vlan mapping table WORD

3.8.7 dot1q ethertype
Command Purpose
Use this command to set ethertype on interface.
Command Syntax

```
dot1q ethertype VALUE
no dot1q ethertype
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VALUE</td>
<td>Specify the ethertype of VLAN tag.</td>
<td>The format is HEX, the default value is 0x8100</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

None

**Usage**

None

**Examples**

Set ethertype to 0x9100:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dot1q ethertype 9100
```

**Related Commands**

None

### 3.8.8 show vlan mapping table

**Command Purpose**

Use this command to display current **vlan mapping table**.

**Command Syntax**

```
show vlan mapping table (WORD )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>The vlan mapping table to be displayed</td>
<td>Up to 16 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

This example show all vlan mapping table existed in system:

```
Switch# show vlan mapping table
Table Name | EVC Name   | Mapped VLAN | Forward Interface | Raw VLAN |
-----------|------------|-------------|-------------------|----------|
VMT        | evc_table  | 100         | n/a               | 10-20    |
VMT_double | evc_double  | 10(100)     | n/a               | untagged |
VMT_forward| evc_forward | 20          | eth-0-9           | 30       |
```
Related Commands

show vlan mapping table applied-interface

3.8.9  show vlan mapping table applied-interface

Command Purpose
Use this command to display who is using the vlan mapping table of interface.

Command Syntax
show vlan mapping table applied-interface

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example show which interface used the vlan mapping table:

Switch# show vlan mapping table applied-interface

<table>
<thead>
<tr>
<th>Table Name</th>
<th>Interface Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMT</td>
<td>eth-0-1</td>
<td>802.1Q-Tunnel</td>
</tr>
</tbody>
</table>

Related Commands

show vlan mapping table WORD

3.8.10  switchport mode

Command Purpose
Use this command to configure switchport mode

Command Syntax
switchport mode ( access | trunk | dot1q-tunnel )
no switchport dot1q-tunnel

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>access</td>
<td>Configure this port to access port</td>
<td>-</td>
</tr>
<tr>
<td>trunk</td>
<td>Configure this port to trunk port</td>
<td>-</td>
</tr>
<tr>
<td>dot1q-tunnel</td>
<td>Configure this port to dot1q-tunnel port</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
None
Usage
None

Examples
This example shows how to configure a switchport to dot1q-tunnel port:

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

Related Commands
show interface switchport

### 3.8.11 switchport dot1q-tunnel type

**Command Purpose**
Use this command to configure dot1q-tunnel type.

**Command Syntax**
```
switchport dot1q-tunnel type ( basic | selective )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>basic</td>
<td>Dot1q-tunnel basic type</td>
<td>-</td>
</tr>
<tr>
<td>selective</td>
<td>Dot1q-tunnel selective type</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**
Interface Configuration

**Default**
basic type

**Usage**
None

**Examples**
This command is used to configure dot1q-tunnel type:

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

Related Commands
show interface switchport

### 3.8.12 switchport dot1q-tunnel native

**Command Purpose**
Use this command to configure a switch-port's default vlan.

**Command Syntax**
```
switchport dot1q-tunnel native ( vlan | inner-vlan ) VLAN_ID
no switchport dot1q-tunnel native vlan
```
### Command Mode

**Interface Configuration**

### Default

None

### Usage

None

### Examples

Configure the eth-0-1 to dot1q-tunnel and configure this port's native to vlan 10:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 100
Switch(config-vlan)# exit
Switch(config)# interface eth-0-23
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# switchport dot1q-tunnel native vlan 100
```

### Related Commands

None

#### 3.8.13 switchport dot1q-tunnel allow vlan

### Command Purpose

Use this command to configure dot1q-tunnel allowed vlan.

### Command Syntax

```
switchport dot1q-tunnel allow vlan ( all | none | add VLAN_ID | remove VLAN_ID )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Add all VLANs to the allowed VLAN list</td>
<td></td>
</tr>
<tr>
<td>none</td>
<td>Remove all VLANs from the allowed VLAN list</td>
<td></td>
</tr>
<tr>
<td>add VLAN_ID</td>
<td>Add VLANs to the allowed VLAN list</td>
<td>1-4094</td>
</tr>
<tr>
<td>remove VLAN_ID</td>
<td>Remove VLANs from the allowed VLAN list</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

### Command Mode

**Interface Configuration**

### Default

None
Usage
None

Examples
Configure dot1q-tunnel allowed vlan 100 on interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport dot1q-tunnel allowed vlan add 100
```

Related Commands
show vlan brief

3.8.14 switchport dot1q-tunnel vlan mapping table

Command Purpose
Use this command to apply vlan mapping table on selective dot1q tunnel port.

Command Syntax
```
switchport dot1q-tunnel vlan mapping table WORD
no switchport dot1q-tunnel vlan mapping table
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>VLAN mapping table name</td>
<td>Up to 16 characters</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
None

Usage
Apply exist vlan mapping table on dot1q-tunnel port. The type of dot1q-tunnel port should be selective.

Examples
The following is a sample that applying vlan mapping table on selective dot1q tunnel port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport dot1q-tunnel vlan mapping table mp
```

Related Commands
show interface switchport

3.8.15 switchport dot1q-tunnel vlan mapping miss-forward

Command Purpose
Use this command to set packet do normal forward when vlan mapping table is not matched on selective dot1q tunnel port.

Command Syntax
```
switchport dot1q-tunnel vlan mapping miss-forward
no switchport dot1q-tunnel vlan mapping miss-forward
```
Command Mode
Interface Configuration

Default
None

Usage
Need to switch the dot1q-tunnel port in selective type before config this command.

Examples
The following is a sample that set packet do normal forward when vlan mapping table is not matched on selective dot1q tunnel port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport dot1q-tunnel vlan mapping miss-forward
```

Related Commands

3.8.16 switchport trunk vlan-translation

Command Purpose
Use this command to enable vlan translation.

Command Syntax
```
switchport trunk vlan-translation
no switchport trunk vlan-translation
```

Command Mode
Interface Configuration

Default
None

Usage
Use this command to enable vlan translation on trunk port. Only trunk port can enable vlan translation.

Examples
The following is a sample that enabling vlan translation on trunk port:

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

Related Commands
show interface switchport

3.8.17 switchport trunk vlan-translation mapping table

Command Purpose
Use this command to apply vlan mapping table on vlan translation port.

Command Syntax
```
switchport trunk vlan-translation mapping table WORD
no switchport trunk vlan-translation mapping table
```
Parameter | Parameter Description | Parameter Value
--- | --- | ---
WORD | VLAN mapping table name | Up to 16 characters

**Command Mode**
Interface Configuration

**Default**
None

**Usage**
Use this command to apply vlan mapping on vlan translation port.

**Examples**
The following is a sample that applying vlan mapping on vlan translation port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport trunk vlan-translation vlan mapping table map_table
```

**Related Commands**
show interface switchport

---

**3.8.18 switchport trunk vlan-translation miss-forward**

**Command Purpose**
Use this command to allow the packet which not match vlan mapping table forward

**Command Syntax**

```
switchport trunk vlan-translation mapping miss-forward
no switchport trunk vlan-translation mapping miss-forward
```

**Command Mode**
Interface Configuration

**Default**
None

**Usage**
None

**Examples**
The following is a sample that let the packet which not matched vlan mapping table forward:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport trunk vlan-translation mapping miss-forward
```

**Related Commands**

---

**3.8.19 vlan dot1q tag native**

**Command Purpose**
Use this command to set tag the vlan on packet if in default vlan
Command Syntax
- vlan dot1q tag native
- no vlan dot1q tag native

Command Mode
Interface Configuration

Default
None

Usage
None

Examples
The following is a sample that tag the vlan if in default vlan:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# vlan dot1q tag native

Related Commands
None

3.8.20 show resource vlan-mapping

Command Purpose
Use this command to display the resource statistic used by vlan mapping table.

Command Syntax
- show resource vlan-mapping

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following is sample output from the show resource vlan-mapping command:

Switch# show resource vlan-mapping

<table>
<thead>
<tr>
<th>VLAN-MAPPING Resource</th>
<th>Used</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applied VLAN Mapping Entry</td>
<td>0</td>
<td>1024</td>
</tr>
</tbody>
</table>

Related Commands
None
3.9 MSTP Commands

3.9.1 spanning-tree enable

Command Purpose
Use this command to enable the Spanning Tree Protocol on a bridge. Use the no parameter to disable the Spanning Tree Protocol on the bridge.

Command Syntax
spanning-tree enable
no spanning-tree enable

Command Mode
Global Configuration

Default
Disable

Usage
None

Examples
This example shows how to global enable stp:

Switch# configure terminal
Switch(config)# spanning-tree enable

This example shows how to global disable stp:

Switch# configure terminal
Switch(config)# no spanning-tree enable

Related Commands
show spanning-tree

3.9.2 spanning-tree priority

Command Purpose
Use this command to set the bridge priority for the common instance for the default bridge. Using a lower priority indicates a higher likelihood of the bridge becoming root. Use the no parameter with this command to reset it to the default value.

Command Syntax
spanning-tree priority PRIORITY
no spanning-tree priority

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRIORITY</td>
<td>Bridge priority</td>
<td>0-61440</td>
</tr>
</tbody>
</table>

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

3.9.3 spanning-tree instance priority

Command Purpose

Use this command to set the default bridge priority for an MST instance to the value specified. Use the no parameter with this command to restore the default value of the default bridge priority.

Command Syntax

```
spanning-tree instance INSTANCE_ID priority PRIORITY
no spanning-tree instance INSTANCE_ID priority
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE_ID</td>
<td>Specify the instance ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>PRIORITY</td>
<td>Specify the bridge priority</td>
<td>0-61440</td>
</tr>
</tbody>
</table>

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

3.9.4 spanning-tree forward-time

Command Purpose

Use this command to set the time after which (if this bridge is the root bridge) each port in the default bridge changes states to learning and forwarding. This value is used by all instances. Use the no parameter with this command to restore the default value of 15 seconds.

Command Syntax

```
spanning-tree forward-time SECONDS
no spanning-tree forward-time
```

show spanning-stree
**Parameter** | **Parameter Description** | **Parameter Value**
--- | --- | ---
SECONDS | Forwarding time delay, in seconds, for the default bridge | 2018/4/30

**Command Mode**
Global Configuration

**Default**
The default value is 15 seconds

**Usage**
The allowable range for the forward time is 4-30 seconds. It is not advisable to set the value below 7 seconds.

**Examples**
This example shows how to set the forward time to 16 seconds:

```
Switch# configure terminal
Switch(config)# spanning-tree forward-time 16
```

This example shows how to reset the forward time to default value:

```
Switch# configure terminal
Switch(config)# no spanning-tree forward-time
```

**Related Commands**
show spanning-tree

---

### 3.9.5 spanning-tree hello-time

**Command Purpose**
Use this command to set the hello-time, the time in seconds after which (if this bridge is the root bridge) all the default bridges in a bridged LAN exchange Bridge Protocol Data Units (BPDUs). A very low value of this parameter leads to excessive traffic on the network, while a higher value delays the detection of topology change. This value is used by all instances.

**Command Syntax**
```
spanning-tree hello-time SECONDS
no spanning-tree hello-time
```

**Parameter** | **Parameter Description** | **Parameter Value**
--- | --- | ---
SECONDS | Hello BPDU interval | 1-10, unit: second

**Command Mode**
Global Configuration

**Default**
The default hello-time value is 2

**Usage**
The allowable range of values is 1-10 seconds.

**Examples**
This example shows how to set the hello time to 5 seconds:

```
Switch# configure terminal
Switch(config)# spanning-tree hello-time 5
```

This example shows how to reset the hello-time to default value:

```
Switch# configure terminal
Switch(config)# no spanning-tree hello-time
```
3.9.6 spanning-tree max-age

Command Purpose
Use this command to set the maximum age for the default bridge. Use the no parameter with this command to restore the default value of the maximum age.

Command Syntax
spanning-tree max-age SECONDS
no spanning-tree max-age

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>The maximum time, in seconds, to listen for the root bridge</td>
<td>6-40</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
The default value of bridge maximum age is 20 seconds.

Usage
Maximum age is the maximum time for which (if a bridge is the root bridge) a message is considered valid. This prevents the frames from looping indefinitely. The value of maximum age should be greater than twice the value of hello time plus 1, and less than twice the value of forward delay minus 1. The allowable range for maximum age is 6-40 seconds. Configure this value sufficiently high, so that a frame generated by root can be propagated to the leaf nodes without exceeding the maximum age.

Examples
This example shows how to set the max age to 12 seconds:

Switch# configure terminal
Switch(config)# spanning-tree max-age 12

This example shows how to reset the max age to default value:

Switch# configure terminal
Switch(config)# no spanning-tree max-age

Related Commands
show spanning-tree

3.9.7 spanning-tree max-hops

Command Purpose
Use this command to specify the maximum allowed hops for a BPDU in an MST region. This parameter is used by all the instances of the MST. To restore the default value, use the no parameter with this command.

Command Syntax
spanning-tree max-hops NUMBER
no spanning-tree max-hops

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>Max hops</td>
<td>1-40</td>
</tr>
</tbody>
</table>
Command Mode
Global Configuration

Default
The default maximum hops in an MST region are 20

Usage
Specifying the maximum hops for a BPDU prevents the messages from looping indefinitely in the network. When a bridge receives an MST BPDU that has exceeded the allowed maximum hops, it discards the BPDU packets.

The configuration should be shown when the bridge is MSTP mode.

Examples
This example shows how to set the max hops to 25:

Switch# configure terminal
Switch(config)# spanning-tree max-hops 25

This example shows how to reset the max hops to default value:

Switch# configure terminal
Switch(config)# no spanning-tree max-hops

Related Commands
show spanning-tree

3.9.8 spanning-tree transmit-holdcount

Command Purpose
Use this command to set the maximum number of transmissions of BPDUs in an MST region by the transmit state machine. Use the no parameter with this command to restore the default transmit hold-count value.

Command Syntax
spanning-tree transmit-holdcount NUMBER
no spanning-tree transmit-holdcount

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>Transmit hold-count value</td>
<td>1-10</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
Transmit hold-count default value is 3

Usage
None

Examples
This example shows how to set hold count to 5:

Switch# configure terminal
Switch(config)# spanning-tree transmit-holdcount 5

This example shows how to reset the hold count to default value:

Switch# configure terminal
Switch(config)# no spanning-tree transmit-holdcount
Related Commands
show spanning-tree

3.9.9 spanning-tree edgeport bpdu-guard

Command Purpose
Use this command to enable the BPDU (Bridge Protocol Data Unit) Guard feature on a bridge. Use the no parameter with this command to disable the BPDU Guard feature on a bridge.

Command Syntax
spanning-tree edgeport bpdu-guard
no spanning-tree edgeport bpdu-guard

Command Mode
Global Configuration

Default
BPDU guard is disabled

Usage
Use the show spanning-tree command to display the bridge and port configurations for the BPDU Guard feature. It shows both the administratively configured and currently running values of the BPDU guard.

Examples
This example shows how to global enable bpdu-guard and enable bpdu-guard on eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree edgeport
Switch(config-if)# spanning-tree edgeport bpdu-guard enable
```

Related Commands
show spanning-tree interface

3.9.10 spanning-tree edgeport bpdu-filter

Command Purpose
Use this command to enable the edgeport BPDU filter for the bridge. Use the no parameter with this command to disable the BPDU filter for the bridge.

Command Syntax
spanning-tree edgeport bpdu-filter
no spanning-tree edgeport bpdu-filter

Command Mode
Global Configuration

Default
None

Usage
Use the show spanning tree command to display administratively configured, and currently running values, of the BPDU filter parameter for the bridge and port.

If bpdu-guard and bpdu-filter are all configured on port, bpdu-filter has a higher priority.
Examples
This example shows how to global enable bpdu-filter and enable bpdu-filter on eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree edgeport
Switch(config-if)# spanning-tree edgeport bpdu-filter
```

Related Commands
show spanning-tree interface

### 3.9.11 spanning-tree port

**Command Purpose**
Use this command to enable or disable spanning tree protocol on specified port.

**Command Syntax**
```
spanning-tree port (enable | disable)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enable spanning protocol on this port</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>Disable spanning protocol on this port</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**
Interface Configuration

**Default**
The default spanning tree state of the port is enabled.

**Usage**
None

**Examples**
This example shows how to enable STP on port eth-0-1:
```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree port enable
```

This example shows how to disable STP on port eth-0-1:
```
Switch# configure terminal
Switch(config-if)# spanning-tree port disable
```

**Related Commands**
show spanning-tree interface

### 3.9.12 spanning-tree port-priority

**Command Purpose**
Use this command to set the port priority for a bridge. A lower priority indicates a greater likelihood of the bridge becoming root.

**Command Syntax**
```
spanning-tree port-priority PRIORITY
no spanning-tree port-priority
```
### Command: `spanning-tree port-priority` - Set Port Priority

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRIORITY</td>
<td>Port priority</td>
<td>0-240</td>
</tr>
</tbody>
</table>

**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`

### Command: `spanning-tree pathcost-standard` - Set Path Cost 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 )`

```
show spanning-tree pathcost-standard
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1d-1998</td>
<td>IEEE 802.1D-1998 standard</td>
<td>-</td>
</tr>
<tr>
<td>dot1t</td>
<td>IEEE 802.1T standard</td>
<td>-</td>
</tr>
</tbody>
</table>

**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
```

**Related Commands**
`show spanning-tree`
3.9.14 spanning-tree path-cost

Command Purpose
Use this command to set the cost of a path associated with the default bridge-group. The lower the path cost, the greater likelihood of the bridge becoming root. Use the no parameter with this command to calculate path cost according to interface's speed.

Command Syntax
spanning-tree path-cost NUMBER
no spanning-tree path-cost

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>The cost to be assigned to the group.</td>
<td>The range is 1 to 200000000 for dot1t and 1-65535 for dot1d-1998</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
The default path cost value is calculated according to interface's speed

Usage
None

Examples
This example shows how to set the STP path-cost to 123:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree path-cost 123
```

This example shows how to reset the STP path-cost to default value:

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

Related Commands
show spanning-tree interface

3.9.15 spanning-tree link-type

Command Purpose
Use this command to enable or disable point-to-point or shared link types. Use the no parameter with this command to disable rapid transition.

Command Syntax
spanning-tree link-type ( auto | point-to-point | shared )
no spanning-tree link-type

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Automatically detect link type</td>
<td>-</td>
</tr>
<tr>
<td>point-to-point</td>
<td>Enable point to point link</td>
<td>-</td>
</tr>
<tr>
<td>shared</td>
<td>Disable point to point link</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration
**Default**
The link type is auto detected

**Usage**
None

**Examples**
This example shows how to set the link type to shared on port eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree link-type shared
```

**Related Commands**
show spanning-tree brief

### 3.9.16 spanning-tree edgeport

**Command Purpose**
Use this command to set a port as an edge-port and to enable rapid transitions. Use the no parameter with this command to set a port to its default state (not an edge-port) and to disable rapid transitions.

**Command Syntax**
```
spanning-tree edgeport
no spanning-tree edgeport
```

**Command Mode**
Interface Configuration

**Default**
The port is not an edge-port

**Usage**
None

**Examples**
This example shows how to set the port eth-0-1 to edgeport:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree edgeport
```

This example shows how to reset the port to an non-edgeport:

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

**Related Commands**
show spanning-tree interface

### 3.9.17 spanning-tree edgeport bpdu-guard

**Command Purpose**
Use this command to enable or disable the BPDU Guard feature on a port. Use the no parameter with this command to set the BPDU Guard feature on a port to default.

**Command Syntax**
```
spanning-tree edgeport bpdu-guard ( enable | disable | default )
```
no spanning-tree edgeport bpdu-guard

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enable edgeport bpdu-guard</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>Disable edgeport bpdu-guard</td>
<td>-</td>
</tr>
<tr>
<td>default</td>
<td>Default</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

BPDU guard is disabled on port

**Usage**

None

**Examples**

This example shows how to change port to edgeport and enable bpdu-guard on port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree edgeport
Switch(config-if)# spanning-tree edgeport bpdu-guard enable
```

**Related Commands**

show spanning tree interface

**3.9.18 spanning-tree edgeport bpdu-filter**

**Command Purpose**

Use this command to set edgeport BPDU filter for the port. Use the no parameter with this command to revert the port BPDU filter value to default.

**Command Syntax**

spanning-tree edgeport bpdu-filter ( enable | disable | default )

no spanning-tree edgeport bpdu-filter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enable edgeport bpdu-filter</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>Disable edgeport bpdu-filter</td>
<td>-</td>
</tr>
<tr>
<td>default</td>
<td>Default</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

BPDU filter is disabled on port

**Usage**

None

**Examples**

This example shows how to enable bpdu-filter on port:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree edgeport
Switch(config-if)# spanning-tree edgeport bpdu-filter

This example shows how to disable bpdu-filter on port:
Switch# configure terminal
Switch(config-if)# no spanning-tree edgeport bpdu-filter

Related Commands
show spanning tree interface

3.9.19 spanning-tree guard root

Command Purpose
Use this command to enable the Root Guard feature for the port. This feature disables reception of superior BPDUs. Use the no parameter with this command to disable the root guard feature for the port.

Command Syntax
spanning-tree guard root
no spanning-tree guard root

Command Mode
Interface Configuration

Default
Root guard is disabled

Usage
The Root Guard feature makes sure that the port on which it is enabled is a designated port. If a port with Root Guard enabled receives a superior BPDU, it goes to a Listening state (for STP) or discarding state (for RSTP and MSTP).

Examples
This example shows how to enable the Root Guard feature for the port:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree guard root

This example shows how to disable the Root Guard feature for the port:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no spanning-tree guard root

Related Commands
None

3.9.20 spanning-tree guard loop

Command Purpose
Use this command to enable the loop guard feature for the port. This feature provides additional protection against Layer 2 forwarding loops. Use the no parameter with this command to disable the loop guard feature for the port.

Command Syntax
spanning-tree guard loop
no spanning-tree guard loop
**Command Mode**

**Interface Configuration**

**Default**

Loop guard is disabled

**Usage**

The loop guard feature should be enabled on the non-designated ports. When a port enables loop guard, and BPDUs are not received on a non-designated port after max_age, the port should move into the STP loop-inconsistent blocking state, instead of the listening / learning / forwarding state, and should not pass user traffic.

**Examples**

This example shows how to enable the loop guard on the port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree guard loop
```

**Related Commands**

spanning-tree guard root

---

### 3.9.21 spanning-tree force-version

**Command Purpose**

Use this command to specify the version. A version identifier of less than a value of 2 enforces the spanning tree protocol. Although the command supports an input range of 0-3, for RSTP, the valid range is 0-2. Use the no parameter with this command to set the default protocol version.

**Command Syntax**

spanning-tree force-version NUMBER

no spanning-tree force-version

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>Version identifier.</td>
<td>0 - STP, 1 - Not supported, 2 - RSTP, 3 - MSTP</td>
</tr>
</tbody>
</table>

**Command Mode**

**Interface Configuration**

**Default**

STP default 0, RSTP default 2, MSTP default 3

**Usage**

None

**Examples**

This example shows how to specify the version:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree force-version 1
```

This example shows how to reset the default version:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no spanning-tree force-version
```

**Related Commands**

None
3.9.22 spanning-tree restricted-tcn

Command Purpose
Use this command to set the restricted TCN value of the port to TRUE. Use the no parameter with this command to set the restricted TCN value of the port to FALSE.

Command Syntax
spanning-tree restricted-tcn
no spanning-tree restricted-tcn

Command Mode
Interface Configuration

Default
The default restricted TCN value is FALSE

Usage
None

Examples
This example shows how to set the restricted TCN value of the port to TRUE:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree restricted-tcn
```

This example shows how to set the restricted TCN value of the port to FALSE:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no spanning-tree restricted-tcn
```

Related Commands
None

3.9.23 spanning-tree restricted-role

Command Purpose
Use this command to set the restricted-role value of the port to TRUE. Use the no parameter with this command to set the restricted-role value of the port to FALSE.

Command Syntax
spanning-tree restricted-role
no spanning-tree restricted-role

Command Mode
Interface Configuration

Default
The default restricted-role value is FALSE

Usage
None

Examples
This example shows how to set the restricted-role value of the port to TRUE:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree restricted-role
```
This example shows how to set the restricted-role value of the port to FALSE:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no spanning-tree restricted-role
```

**Related Commands**

None

### 3.9.24 spanning-tree tc-protection

**Command Purpose**

Use this command to set the tc-protection value to TRUE. Use the no parameter with this command to set the tc-protection value to FALSE. If tc-protection is set, the number of tc packets which can be processed every hello time interval shouldn't be greater than the number of tc-protection threshold.

**Command Syntax**

- spanning-tree tc-protection
- no spanning-tree tc-protection

**Command Mode**

Global Configuration

**Default**

The default tc-protection value is FALSE

**Usage**

None

**Examples**

This example shows how to set the tc-protection value to TRUE:

```
Switch# configure terminal
Switch(config)# spanning-tree tc-protection
```

This example shows how to set the tc-protection value to FALSE:

```
Switch# configure terminal
Switch(config)# no spanning-tree tc-protection
```

**Related Commands**

None

### 3.9.25 spanning-tree tc-protection threshold

**Command Purpose**

Use this command to set the tc-protection threshold value. Use the no parameter with this command to set the tc-protection threshold value to 1. If tc-protection is set, the number of tc packets which can be processed every hello time interval shouldn't be greater than the number of tc-protection threshold.

**Command Syntax**

- spanning-tree tc-protection threshold NUMBER
- no spanning-tree tc-protection threshold

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>Tc-protection threshold value, default 1</td>
<td>1-255</td>
</tr>
</tbody>
</table>
Command Mode
Global Configuration

Default
The default tc-protection threshold value is 1

Usage
None

Examples
This example shows how to set the tc-protection to 255:

```
Switch# configure terminal
Switch(config)# spanning-tree tc-protection threshold 255
```

This example shows how to reset the tc-protection to default value:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no spanning-tree tc-protection threshold
```

Related Commands
None

3.9.26 spanning-tree mode

Command Purpose
Use this command to set spanning tree mode.

Command Syntax
```
spanning-tree mode ( stp | rstp | mstp )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>stp</td>
<td>spanning tree protocol</td>
<td>-</td>
</tr>
<tr>
<td>rstp</td>
<td>rapid spanning tree protocol</td>
<td>-</td>
</tr>
<tr>
<td>mstp</td>
<td>multiple spanning tree protocol</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
The default spanning-tree mode is stp

Usage
None

Examples
This example shows how to set the spanning tree mode to mstp:

```
Switch# configure terminal
Switch(config)# spanning-tree mode mstp
```

Related Commands
None
3.9.27 spanning-tree instance port-priority

Command Purpose
Use this command to set the port priority for a bridge group. Use the no parameter with this command to restore the default priority value.

Command Syntax
spanning-tree instance INSTANCE_ID port-priority PRIORITY
no spanning-tree instance INSTANCE_ID port-priority

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE_ID</td>
<td>Specify the identifier</td>
<td>1-4094</td>
</tr>
<tr>
<td>PRIORITY</td>
<td>Specify the port priority (a lower priority indicates greater likelihood of the interface becoming a root). The range is 0-240</td>
<td>0-240</td>
</tr>
</tbody>
</table>

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

3.9.28 spanning-tree instance path-cost

Command Purpose
Use this command to set the cost of a path associated with an interface. Use the no parameter with this command to restore the default cost value of the path.

Command Syntax
spanning-tree instance INSTANCE_ID path-cost COST
no spanning-tree instance INSTANCE_ID path-cost
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE_ID</td>
<td>Specify the identifier</td>
<td>1-4094</td>
</tr>
<tr>
<td>COST</td>
<td>Specify the cost of path</td>
<td>(&lt;1-200000000&gt;) for dot1t and (&lt;1-65535&gt;) for dot1d-1998 (a lower path-cost indicates a greater likelihood of the specified interface becoming a root)</td>
</tr>
</tbody>
</table>

**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-if)# exit
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 3
Switch(config-if)# spanning-tree instance 3 path-cost 1000
```

**Related Commands**

None

### 3.9.29 spanning-tree instance restricted-tcn

**Command Purpose**

Use this command to set the restricted TCN value for the instance to TRUE. Use the no parameter with this command to set the restricted TCN value for the instance to FALSE.

**Command Syntax**

```
spanning-tree instance INSTANCE_ID restricted-tcn
no spanning-tree instance INSTANCE_ID restricted-tcn
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE_ID</td>
<td>Specify the instance ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

The default restricted TCN value is FALSE
### Usage

None

### Examples

This example shows how to set the restricted TCN value for the instance to TRUE:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree instance 2 restricted-tcn
```

### Related Commands

None

#### 3.9.30 spanning-tree instance restricted-role

**Command Purpose**

Use this command to set the restricted role value for the instance to TRUE. Use the no parameter with this command to set the restricted role value for the instance to FALSE.

**Command Syntax**

```
spanning-tree instance INSTANCE_ID restricted-role

no spanning-tree instance INSTANCE_ID restricted-role
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE_ID</td>
<td>Specify the instance ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

The default restricted-role value is FALSE.

**Usage**

None

**Examples**

This example shows how to set the restricted role value for the instance to TRUE:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree instance 2 restricted-role
```

**Related Commands**

None

#### 3.9.31 spanning-tree mst configuration

**Command Purpose**

Use this command to enter mst configuration mode.

**Command Syntax**

```
spanning-tree mst configuraiton
```

**Command Mode**

Global Configuration
Default
None

Usage
None

Examples
This example shows how to enter into mst configuration mode:

Switch# configure terminal
Switch(config)# spanning-tree mst configuration

Related Commands
None

3.9.32 instance

Command Purpose
Use this command to create an mstp instance and map VLANs to an MST instance.

Command Syntax
instance INSTANCE_ID vlan VLAN_ID
no instance INSTANCE_ID vlan VLAN_ID

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE_ID</td>
<td>Instance id, we support at most 64 instances</td>
<td>1-4094</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>The vlan associated with instance must be created first</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode
MST Configuration

Default
None

Usage
When you map VLANs to an MST instance, the mapping is incremental, and the VLANs specified in the command are added to or removed from the VLANs that were previously mapped.

Examples
This example shows how to map vlan 10 to instance 1:

Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 10
Switch(config-vlan)# exit
Switch(config)# spanning-tree Mst configuration
Switch(config-mst)# instance 1 vlan 10

Related Commands
None
3.9.33  region

Command Purpose
Use this command to create mstp region.

Command Syntax
region NAME
no region NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Specify the region name.</td>
<td>The name string has a maximum length of 32 characters and is case sensitive</td>
</tr>
</tbody>
</table>

Command Mode
MST Configuration

Default
The default region name is an empty string

Usage
None

Examples
This example shows how to set the region to Switch:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 10
Switch(config-vlan)# exit
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# region Switch
```

Related Commands
None

3.9.34  revision

Command Purpose
Use this command to create an mstp revision number.

Command Syntax
revision NUMBER
no revision NUMBER

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>Specify the configuration revision number.</td>
<td>0-65535</td>
</tr>
</tbody>
</table>

Command Mode
MST Configuration

Default
Default value is 0
Usage
None

Examples
This example shows how to set the revision number to 1:

Switch# configure terminal
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# revision 1

Related Commands
None

3.9.35 clear spanning-tree detected protocols

Command Purpose
Use this command to clear the detected protocols for a specific bridge or interface.

Command Syntax
clear spanning-tree detected protocols (interface IFNAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface IFNAME</td>
<td>Specify the name of the interface on which protocols have to be cleared</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to clear the detected protocols for a specific bridge or interface eth-0-1:

Switch# clear spanning-tree detected protocols interface eth-0-1

Related Commands
None

3.9.36 clear spanning-tree disabled-port

Command Purpose
Use this command to clear all spanning tree protocol disabled port.

Command Syntax
clear spanning-tree disabled-port

Command Mode
Privileged EXEC

Default
None
Usage
None

Examples
This example shows how to clear all spanning tree protocol disabled port:

```
Switch# clear spanning-tree disabled-port
```

Related Commands
None

3.9.37 show spanning-tree

Command Purpose
Use this command to show the state of the spanning tree. This command only shows up interface's state.

Command Syntax
```
show spanning-tree
```

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to show the state of spanning tree:

```
Switch# show spanning-tree
Bridge up - Spanning Tree Enabled
Mode - Multiple spanning tree protocol
Path Cost Standard - dot1t
CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
Tx Hold Count 6
CIST Root Id 80008afa58e9cb00
CIST Reg Root Id 80008afa58e9cb00
CIST Bridge Id 80008afa58e9cb00
Edgeport bpdu-filter disabled
Edgeport bpdu-guard disabled
eth-0-1: Port 1 - Id 8001 - Role Designated - State Forwarding
eth-0-1: Designated External Path Cost 0 - Internal Path Cost 0
eth-0-1: Configured Path Cost 20000 - Add type Explicit ref count 1
eth-0-1: Designated Port Id 8001 - CIST Priority 128
eth-0-1: CIST Root 80008afa58e9cb00
eth-0-1: Regional Root 80008afa58e9cb00
eth-0-1: Designated Bridge 80008afa58e9cb00
eth-0-1: Message Age 0 - Max Age 20
eth-0-1: CIST Hello Time 2 - Forward Delay 15
eth-0-1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
eth-0-1: Forward-transitions 2
eth-0-1: BPDU sent 373 - BPDU received 0
eth-0-1: Version Multiple spanning tree protocol - Received None - Send MSTP
eth-0-1: No edgeport configured - Current edgeport off
eth-0-1: Edgeport bpdu-guard Default - Current edgeport bpdu-guard off
eth-0-1: Edgeport bpdu-filter Default - Current edgeport bpdu-filter off
eth-0-1: No root guard configured - Current root guard off
eth-0-1: No loop guard configured - Current loop guard off
eth-0-1: Configured Link Type auto - Current point-to-point
```
Related Commands

None

3.9.38 show spanning-tree interface

Command Purpose

Use this command to show the state of the spanning tree of the specified interface.

Command Syntax

show spanning-tree interface IFNAME (brief )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Specify the name of the interface</td>
<td>-</td>
</tr>
<tr>
<td>brief</td>
<td>The brief spanning-tree information</td>
<td>-</td>
</tr>
</tbody>
</table>

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 timer 0
eth-0-1: Forward-transitions 2
eth-0-1: BPDU sent 352 - BPDU received 0
eth-0-1: Version Multiple spanning tree protocol - Received None - Send MSTP
eth-0-1: No edgeport configured - Current edgeport off
eth-0-1: Edgeport bpdu-guard Default - Current edgeport bpdu-guard off
eth-0-1: Edgeport bpdu-filter Default - Current edgeport bpdu-filter off
eth-0-1: No root guard configured - Current root guard off
eth-0-1: No loop guard configured - Current loop guard off
eth-0-1: Configured Link Type auto - Current point-to-point
Related Commands
None

3.9.39 show spanning-tree brief

Command Purpose
Use this command to show the brief state of the spanning tree.

Command Syntax
show spanning-tree brief

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following is an output of this command displaying the brief state of the spanning tree. The down interface should not be show:

```
Switch# show spanning-tree brief
Multiple spanning tree protocol Enabled
Root ID Priority 32768 (0x8000)
  Address 8afa.58e9.cb00
  Hello Time 2 sec
  Max Age 20 sec
  Forward Delay 15 sec
Bridge ID Priority 32768 (0x8000)
  Address 8afa.58e9.cb00
  Hello Time 2 sec
  Max Age 20 sec
  Forward Delay 15 sec
  Aging Time 300 sec
Interface Role State Cost Priority Number Type
----------------- -------------------- ---- ------ ------
eth-0-1 Designated Forwarding 20000 128.1 P2p
eth-0-2 Designated Forwarding 20000 128.2 P2p
```

Related Commands
None

3.9.40 show spanning-tree disabled-port

Command Purpose
Use this command to show the spanning tree protocol disabled port.

Command Syntax
show spanning-tree disabled-port

Command Mode
Privileged EXEC

Default
None

Usage
None
Examples

The following is an output of this command displaying all spanning tree protocol disabled port:

```
Switch# show spanning-tree disabled-port
Interface  ---------
    eth-0-1
```

Related Commands

None

3.9.41 show spanning-tree mst

Command Purpose

Use this command to show the mstp information.

Command Syntax

```
show spanning-tree mst
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is an output of this command displaying the mstp information. The down interface should not be show:

```
Switch#show spanning-tree mst
Bridge up - Spanning Tree Enabled
    Mode - Multiple spanning tree protocol
    Path Cost Standard - dot1t
    CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
    Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
    Tx Hold Count 6
    CIST Root Id 80008fa58e9cb00
    CIST Reg Root Id 80008fa58e9cb00
    CIST Bridge Id 80008fa58e9cb00
    Edgeport bpdu-filter disabled
    Edgeport bpdu-guard disabled

Instance Interface VLAN
0: eth-0-2 1, 3
1: eth-0-2 2
```

Related Commands

None

3.9.42 show spanning-tree mst config

Command Purpose

Use this command to show the mstp region configuration information.

Command Syntax

```
show spanning-tree mst config
```
**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
This example shows how to show the mstp region configuration information:

Switch#show spanning-tree mst config

MSTP Configuration Information:

<table>
<thead>
<tr>
<th>Format Id</th>
<th>: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>: switch</td>
</tr>
<tr>
<td>Revision Level</td>
<td>: 0</td>
</tr>
<tr>
<td>Digest</td>
<td>: 0x3AB68794D602FDF43B21C0B37AC38CA8</td>
</tr>
<tr>
<td>Instances configured</td>
<td>: 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Instance</th>
<th>Vlans mapped</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1, 3</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

**Related Commands**
None

---

3.9.43 show spanning-tree mst detail

**Command Purpose**
Use this command to show the detail mstp information.

**Command Syntax**
show spanning-tree mst detail ( interface IFNAME )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface IFNAME</td>
<td>The interface name you want to display</td>
<td>-</td>
</tr>
</tbody>
</table>

**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
3.9.44 show spanning-tree mst instance

Command Purpose
Use this command to show the detail mstp information of a specific instance.

Command Syntax
show spanning-tree mst instance INSTANCE_ID ( interface IFNAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE_ID</td>
<td>Instance number you want to display</td>
<td>1-4094</td>
</tr>
<tr>
<td>IFNAME</td>
<td>The interface name you want to display</td>
<td>Support physical/aggregation ports</td>
</tr>
</tbody>
</table>

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
Related Commands

None

3.9.45  show spanning-tree mst interface

Command Purpose

Use this command to show the detail mstp information of a specific interface.

Command Syntax

show spanning-tree mst interface IFNAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>The interface name you want to display</td>
<td>Support physical/aggregation ports</td>
</tr>
</tbody>
</table>

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
3.9.46 show spanning-tree mst brief

**Command Purpose**
Use this command to show the brief mstp information.

**Command Syntax**

```
show spanning-tree mst brief ( interface IFNAME | instance INSTANCE_ID )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface IFNAME</td>
<td>The interface name you want to display</td>
<td>-</td>
</tr>
<tr>
<td>instance INSTANCE_ID</td>
<td>Instance number you want to display</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

**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
--------------------
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
3.9.47 spanning-tree instance forward

Command Purpose
Use this command to set STP state is forward for instance and keep forward.

Command Syntax
spanning-tree instance INSTANCE_ID forward
no spanning-tree instance INSTANCE_ID forward

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE_ID</td>
<td>Specify the identifier</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

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-mst)# interface eth-0-1
Switch(config-if)# spanning-tree instance 1 forward
Switch# configure terminal
Switch(config)# interface eth-0-1
```

Related Commands

3.10 Flow Control Commands

3.10.1 flowcontrol send

Command Purpose
Use this command to enable or disable flow control send function.

Command Syntax
flowcontrol send { on | off }

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Set send flowcontrol enable</td>
<td>-</td>
</tr>
<tr>
<td>off</td>
<td>Set send flowcontrol disable</td>
<td>-</td>
</tr>
</tbody>
</table>

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(config-if)# flowcontrol send on
```

Related Commands
flowcontrol receive on

3.10.2 flowcontrol receive

Command Purpose
Use this command to enable or disable flow control receive function.

Command Syntax
```
flowcontrol receive (on | off )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Set receive flowcontrol enable</td>
<td>-</td>
</tr>
<tr>
<td>off</td>
<td>Set receive flowcontrol disable</td>
<td>-</td>
</tr>
</tbody>
</table>

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(config-if)# flowcontrol receive on
```

Related Commands
flowcontrol send on

3.10.3 show flowcontrol

Command Purpose
Use this command to display flow control information.

Command Syntax
```
show flowcontrol ( IFNAME | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical ports</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Port</th>
<th>Receive FlowControl</th>
<th>Send FlowControl</th>
<th>RxPause</th>
<th>TxPause</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>admin</td>
<td>oper</td>
<td>admin</td>
<td>oper</td>
</tr>
<tr>
<td>eth-0-1</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>eth-0-2</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>eth-0-3</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>eth-0-4</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>eth-0-5</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>eth-0-6</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>eth-0-7</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>eth-0-8</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>eth-0-9</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>eth-0-10</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>eth-0-11</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>eth-0-12</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>eth-0-13</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>eth-0-14</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>eth-0-15</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>eth-0-16</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>eth-0-17</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>eth-0-18</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>eth-0-19</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>eth-0-20</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>eth-0-21</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>eth-0-22</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>eth-0-23</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>eth-0-24</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
</tbody>
</table>

Related Commands
None

3.11 Priority-based Flow Control Commands

3.11.1 priority-flow-control enable priority

Command Purpose
Use this command to enable or disable priority-based flow control function on which priority.

Command Syntax
priority-flow-control enable priority { 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 }
no priority-flow-control enable priority { 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 }

Command Mode
Interface Configuration

Default
Enable priority-based flow control on priority 3
Usage

Use the priority-flow-control enable priority interface Configuration command to set the interface's ability to send pause frames to on or off on which priorities.

Examples

This example shows how to enable priority-based flow control on which priorities:

```
Switch# configure terminal
Switch(config-if)# Priority-flow-control enable priority 2 3 5 7
```

Related Commands

priority-flow-control mode (on | auto)
lldp tlv 8021-org-specific dcbx

### 3.11.2 show priority-flow-control

**Command Purpose**

Use this command to display priority-based flowcontrol information.

**Command Syntax**

`show priority-flow-control (INTERFACE | )`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERFACE</td>
<td>Interface name</td>
<td>Support physical ports</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

Use the command to display priority-based flowcontrol admin-config and operation-config information of each port.

**Examples**

This example shows how to display priority-based flowcontrol information:

```
Switch# show priority-flow-control interface eth-0-1
Switch# show priority-flow-control
```

```
<table>
<thead>
<tr>
<th>Port</th>
<th>PFC-enable admin</th>
<th>PFC-enable admin</th>
<th>PFC-enable oper</th>
<th>PFC-enable oper</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-0-1</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
</tbody>
</table>
```

**Related Commands**

None

### 3.11.3 show priority-flow-control statistics

**Command Purpose**

Use this command to display priority-based flowcontrol statistics.

**Command Syntax**

`show priority-flow-control statistics ( INTERFACE | )`
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERFACE</td>
<td>Interface name</td>
<td>Support physical ports</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
Use the command to display priority-based flowcontrol statistics of each port.

**Examples**
This example shows how to display priority-based flowcontrol statistics:

```
Switch# show priority-flow-control statistics interface eth-0-1
Switch# show priority-flow-control statistics
```

<table>
<thead>
<tr>
<th>Port</th>
<th>RxPause</th>
<th>TxPause</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-0-1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Related Commands**
None

### 3.12 Layer 2 Protocols Tunneling Commands

#### 3.12.1 l2protocol enable

**Command Purpose**
Use this command to enable l2protocol function globally.

**Command Syntax**
```
l2protocol enable
no l2protocol enable
```

**Command Mode**
Global Configuration

**Default**
None

**Usage**
Use this command to enable l2protocol function globally.

**Examples**
This example shows how to enable l2protocol function globally:

```
Switch# configure terminal
Switch(config)# l2protocol enable
```

**Related Commands**
show l2protocol

#### 3.12.2 l2protocol tunnel-dmac

**Command Purpose**
Use this command to configure l2protocol tunnel destination MAC address.

**Command Syntax**

I2protocol tunnel-dmac MAC

no I2protocol tunnel-dmac

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC</td>
<td>l2 protocol tunnel's destination MAC address</td>
<td>0100.0CCD.CDD0-D2 or 010F.E200.0003</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

Default

None

**Usage**

Use this command to configure l2 protocol tunnel dmac. System default tunnel-dmac is 0100.0cc.cdd0.

**Examples**

Following is a sample that configuring 010FE2000003 as l2 protocol tunnel dmac:

Switch# configure terminal
Switch(config)# l2protocol tunnel-dmac 010F.E200.0003

**Related Commands**

show l2protocol

---

### 3.12.3 l2protocol mac 1

**Command Purpose**

Use this command to configure l2 protocol mac address globally.

**Command Syntax**

I2protocol mac 1 MAC mask MASK

no I2protocol mac 1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC</td>
<td>L2 Protocol MAC address. 0180.C200.0000~0180.C200.00 3F is used by other protocol, so this range is out of L2 Protocol MAC address control.</td>
<td>0180.C200.0000 ~ 0180.C2FF.FFFF</td>
</tr>
<tr>
<td>MASK</td>
<td>L2 Protocol MAC MASK</td>
<td>FFFF.FF00.0000 ~ FFFF.FFFFFF</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

Default

None

**Usage**

Use this command to configure l2 protocol mac address globally.

**Examples**
This example shows how to configure L2 protocol mac address:

```
Switch# configure terminal
Switch(config)# l2protocol mac 1 0180.c222.0000 mask ffff.ffff.0000
```

### Related Commands
- `l2protocol full-mac`

#### 3.12.4 l2protocol mac <2-6>

**Command Purpose**
Use this command to configure L2 protocol mac address globally.

**Command Syntax**
- `l2protocol mac MAC_NUM MAC`
- `no l2protocol mac MAC_NUM`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC_NUM</td>
<td>The ID of L2 protocol MAC</td>
<td>2-6</td>
</tr>
<tr>
<td>MAC</td>
<td>The MAC address of L2 protocol MAC</td>
<td>0180.C200.0000 ~ 0180.C2FF.FFFF</td>
</tr>
</tbody>
</table>

**Command Mode**
- Global Configuration

**Default**
None

**Usage**
Use this command to configure L2 protocol mac address globally. Should not overlap each other.

**Examples**
This example shows how to configure L2 protocol mac address:

```
Switch# configure terminal
Switch(config)# l2protocol mac 3 0180.c200.0000
```

**Related Commands**
- `l2protocol full-mac`

#### 3.12.5 l2protocol

**Command Purpose**
Use this command to configure L2 protocol pdu-mac-address to discard, peer or tunnel.

**Command Syntax**
- `l2protocol (stp | slow-proto | dot1x | cfm | mac MAC_NUM | full-mac) ( discard | peer | tunnel ( evc WORD ) | forward )`
- `l2protocol ( cdp | vtp | lldp | all ) ( discard | peer | forward )`
- `no l2protocol ( stp | slow-proto | dot1x | cfm | lldp | cdp | vtp | all | mac MAC_NUM | full-mac )`
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>stp</td>
<td>MAC: 0180.c200.0000</td>
<td>-</td>
</tr>
<tr>
<td>slow-proto</td>
<td>MAC: 0180.c200.0002, ethertype: 0x8809</td>
<td>-</td>
</tr>
<tr>
<td>dot1x</td>
<td>MAC: 0180.c200.0003, ethertype: 0x888e</td>
<td>-</td>
</tr>
<tr>
<td>cfm</td>
<td>ethertype: 0x8902</td>
<td>-</td>
</tr>
<tr>
<td>cdp</td>
<td>Cisco Discovery Protocol</td>
<td>-</td>
</tr>
<tr>
<td>vtp</td>
<td>Vlan Trunking Protocol</td>
<td>-</td>
</tr>
<tr>
<td>lldp</td>
<td>Link Layer Discovery Protocol</td>
<td>-</td>
</tr>
<tr>
<td>all</td>
<td>include stp, slow-proto, dot1x, cfm, lldp, cdp, vtp</td>
<td>-</td>
</tr>
<tr>
<td>mac MAC_NUM</td>
<td>Globally configured mac 1-2</td>
<td>1-2</td>
</tr>
<tr>
<td>discard</td>
<td>Discard the protocol data unit</td>
<td>-</td>
</tr>
<tr>
<td>peer</td>
<td>Act as peer to the customer device instance of the protocol, peer is default option</td>
<td>-</td>
</tr>
<tr>
<td>tunnel</td>
<td>Tunnel the protocol data unit into the SVLAN</td>
<td>-</td>
</tr>
<tr>
<td>forward</td>
<td>Forward the protocol data unit</td>
<td>-</td>
</tr>
<tr>
<td>full-mac</td>
<td>Globally configured full-mac</td>
<td>-</td>
</tr>
<tr>
<td>WORD</td>
<td>The evc name</td>
<td>Up to 15 characters</td>
</tr>
</tbody>
</table>

**Command Mode**
Interface Configuration

**Default**
None

**Usage**
Use this command to configure l2 protocol to discard, peer or tunnel.

**Examples**
This example shows how to configure l2 protocol to discard:
```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# l2protocol stp discard
```
This example shows how to configure l2 protocol to tunnel:
```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# l2protocol slow-proto tunnel evc evc1
```

**Related Commands**
None

### 3.12.6 12protocol uplink enable

**Command Purpose**
Use this command to configure l2 protocol uplink port.
**Command Syntax**

l2protocol uplink enable  
no l2protocol uplink enable

**Command Mode**

Interface Configuration

**Default**

None

**Usage**

Use this command to configure l2 protocol uplink port.

**Examples**

This example shows how to configure l2 protocol uplink port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# l2protocol uplink enable
```

**Related Commands**

None

### 3.12.7 show l2protocol

**Command Purpose**

Use this display current l2 protocol tunnel configuration.

**Command Syntax**

```
show l2protocol (interface IFNAME | tunnel-dmac | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface IFNAME</td>
<td>Interface name</td>
<td>Support aggregation and physical ports</td>
</tr>
<tr>
<td>tunnel-dmac</td>
<td>Layer2 protocols tunnel destination MAC address</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

Use this display current l2 protocol tunnel configuration or on specified interface.

**Examples**

This example shows how to display current l2 protocol tunnel configuration on interface eth-0-1:

```
Switch# show l2protocol interface eth-0-1
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>PDU Address</th>
<th>MASK</th>
<th>Status</th>
<th>EVC</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-0-1</td>
<td>stp</td>
<td>ffffff</td>
<td>Peer</td>
<td>N/A</td>
</tr>
<tr>
<td>eth-0-1</td>
<td>slow-proto</td>
<td>ffffff</td>
<td>Peer</td>
<td>N/A</td>
</tr>
<tr>
<td>eth-0-1</td>
<td>dot1x</td>
<td>ffffff</td>
<td>Peer</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Switch # show l2protocol tunnel-dmac

Layer2 protocols tunnel destination MAC address is 0100.0ccd.cdd0
This example shows how to display current l2 protocol tunnel configuration on tunnel-mac:

Switch# show l2protocol tunnel-dmac

Layer2 protocols tunnel destination MAC address is 0100.0ccd.cdd0

Related Commands
None

3.12.8 l2protocol cos

Command Purpose
Use this command to configure l2protocol cos globally.

Command Syntax
l2protocol cos COS_VALUE
no l2protocol cos

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>COS_VALUE</td>
<td>vlan tag priority</td>
<td>0-7</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
Use this command to configure l2protocol cos globally, the default value is 0.

Examples
This example shows how to configure l2protocol cos 7:

Switch# configure terminal
Switch(config)# l2protocol cos 7

Related Commands
None

3.12.9 l2protocol full-mac

Command Purpose
Use this command to configure l2 protocol mac address globally.

Command Syntax
l2protocol full-mac MAC
no l2protocol full-mac

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC</td>
<td>Destination MAC address, including all MAC addresses</td>
<td>0000.0000.0000 ~ FFFF.FFFF.FFFF</td>
</tr>
</tbody>
</table>
Command Mode
Global Configuration

Default
None

Usage
If the L2 protocol full-mac address coincides with BPDU, Slow proto, EAPOL or MAC<1-4>, the tunnel operation priority is orderly: BPDU, Slow proto, EAPOL, full-mac, mac<1-4>.

If the L2 protocol full-mac address coincides with L2 Protocol tunnel destination MAC address, the crossed L2 protocol mac address won't take effect when tunnel L2 Protocol

Examples
This example shows how to configure l2 protocol full-mac address:

Switch# configure terminal
Switch(config)# l2protocol full-mac 0100.0CCC.CCCC

Related Commands
l2protocol mac

3.13 Storm Control Commands
3.13.1 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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>broadcast</td>
<td>Enable broadcast storm control on the interface</td>
<td>-</td>
</tr>
<tr>
<td>multicast</td>
<td>Enable multicast storm control on the interface</td>
<td>-</td>
</tr>
<tr>
<td>unicast</td>
<td>Enable unicast storm control on the interface</td>
<td>-</td>
</tr>
<tr>
<td>level LEVEL</td>
<td>Specify the rising and falling suppression levels as a percentage of total bandwidth</td>
<td>0.00-100.00</td>
</tr>
<tr>
<td></td>
<td>of the port.</td>
<td></td>
</tr>
<tr>
<td>pps PPS</td>
<td>Specify the rising and falling suppression levels as a rate in packets per second at</td>
<td>0-1000000000</td>
</tr>
<tr>
<td></td>
<td>which traffic is received on the port.</td>
<td></td>
</tr>
</tbody>
</table>

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

3.13.2 show storm-control
Command Purpose
Use this command to show storm-control configurations.

Command Syntax
show storm-control (interface INTERFACE | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface INTERFACE</td>
<td>Interface name</td>
<td>Support physical ports</td>
</tr>
</tbody>
</table>

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

3.13.3 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

### 3.14 Loopback Detection Commands

#### 3.14.1 loopback-detect enable

**Command Purpose**

Using the loopback-detect enable command, you can enable loopback detection on an interface.

Using the no loopback-detect enable command, you can disable loopback detection on an interface. By default, loopback detection is disabled on an interface.

**Command Syntax**

```
loopback-detect enable
no loopback-detect enable
```

**Command Mode**

Interface Configuration

**Default**

Disable

**Usage**

The loopback-detect enable command enables loopback detection on an interface. This function enables the system to detect a loopback on the interface quickly and minimizes impact of the loopback on the entire network. After loopback detection is enabled on an interface, the interface sends loopback detection packets at intervals. Loopback detection occupies CPU resources; therefore, disable this function when it is not required.

**Examples**

This example shows how to enable loopback detect on port eth-0-1:

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

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

**Related Commands**

show loopback-detect
### 3.14.2 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>loopback detect packet send interval</td>
<td>1-300, unit: second</td>
</tr>
</tbody>
</table>

**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`

### 3.14.3 loopback-detect recovery-interval

**Command Purpose**

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

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

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

**Command Syntax**

```
loopback-detect recovery-interval INTERVAL
```

```
no loopback-detect recovery-interval
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>recovery interval in seconds</td>
<td>1-255, unit: second</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration
Default
Recovery-interval is packet-interval * 3

Usage
If the interface is shutdown, this command is useless.

Examples
This example shows how to set the interval for recovering to 10s:

Switch# configure terminal
Switch(config)# loopback-detect recovery-interval 10

Related Commands
show loopback-detect

3.14.4 loopback-detect delay-interval

Command Purpose
Using the loopback-detect delay interval on interface for set action.
Using the no loopback-detect delay-interval to set not delay.

Command Syntax
loopback-detect delay-interval INTERVAL
no loopback-detect delay-interval

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>delay interval</td>
<td>1-255, unit: second</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
None

Usage
The no loopback-detect delay-interval command is used to set on the interface, if received loopback-detect packet, then set action that set on the interface.

Examples
This example shows how to set the interval for delay set action to 5s:

Switch# configure terminal
Switch(config)# loopback-detect delay-interval 5

Related Commands
show loopback-detect

3.14.5 loopback-detect action

Command Purpose
Using the loopback-detect action command, you can configure an action to perform when a loopback is detected on an interface.
Using the no loopback-detect action command, you can restore the default action.
By default, an interface is blocked when a loopback is detected on the interface.
Command Syntax

loopback-detect action { shutdown | trap | block }

no loopback-detect action

Shutdown

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>shutdown</td>
<td>Shuts down an interface when a loopback is detected on the interface.</td>
<td>-</td>
</tr>
<tr>
<td>Trap</td>
<td>Only sends a trap message when a loopback is detected.</td>
<td>-</td>
</tr>
<tr>
<td>block</td>
<td>Block the interface and continue to send loopback-detect packets</td>
<td>-</td>
</tr>
</tbody>
</table>

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

3.14.6 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VID</td>
<td>VLAN ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

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

3.14.7 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 }

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface IFNAME</td>
<td>Show loopback detection status and configuration on interface.</td>
<td>Support physical ports</td>
</tr>
<tr>
<td>packet-interval</td>
<td>Show loopback detect packet interval.</td>
<td>-</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Action</th>
<th>Status</th>
<th>Delay(s)</th>
<th>Recovery(s)</th>
<th>RLeft(s)</th>
<th>Send</th>
<th>Recv</th>
<th>N/A</th>
<th>Count</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-0-47</td>
<td>trap</td>
<td>NORMAL</td>
<td>30</td>
<td>-</td>
<td>15</td>
<td>-</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>eth-0-48</td>
<td>trap</td>
<td>NORMAL</td>
<td>-</td>
<td>15</td>
<td>-</td>
<td>2001-01-05 034721</td>
<td>N/A</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

Related Commands
loopback-detect action
loopback-detect enable
3.15 MLAG Commands

3.15.1 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

3.15.2 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>MLAG peer IPv4 address</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

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

3.15.3 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface for peer link.</td>
<td>Only support phy port or agg port</td>
</tr>
</tbody>
</table>

Command Mode

MLAG Configuration

Default

None

Usage

The peer-link command specifies the interface that connects MLAG peers. To form an MLAG, two switches are connected through an interface called a peer link. The peer link carries control and data traffic between the two switches.

The no peer-link command removes the peer link by deleting the peer-link command from running-config.

Examples

This example shows how to specify the interface that connects MLAG peers:

```
Switch# configure terminal
Switch(config)# mlag configuration
Switch(config-mlag)# peer-link eth-0-9
Switch(config-mlag)#
```

Related Commands

show mlag
3.15.4 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>keepalive</td>
<td>keepalive time interval</td>
<td>1-65535, unit: second</td>
</tr>
<tr>
<td>holdtime</td>
<td>holdtime time interval</td>
<td>4-65535, unit: second</td>
</tr>
</tbody>
</table>

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 keepalive 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

3.15.5 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>period</td>
<td>Disable link interval. The number 0 means that interface not enter into errdisable</td>
<td>0-86400, unit: second</td>
</tr>
<tr>
<td>auto</td>
<td>Auto recovery from errdisable after MLAG peer build successful.</td>
<td>-</td>
</tr>
</tbody>
</table>
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 delay interval:

Switch# configure terminal
Switch(config)# mlag configuration
Switch(config-mlag)# reload-delay 100
Switch(config-mlag)#

Related Commands
show mlag

3.15.6 sync-orphan

Command Purpose
The sync-orphan command specifies the mlag peers to sync MAC entries on orphan port.

The no sync-orphan command disables 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

3.15.7 sync-overlay

Command Purpose
The sync-overlay command specifies the mlag peers to sync MAC entries on overlay logic port.

The no sync-overlay command disable the function.
Command Syntax
sync-overlay
no sync-overlay

Command Mode
MLAG Configuration

Default
Enable

Usage
If this function is disabled, MLAG peers will only sync those MAC entries in MLAG group.

Examples
This example shows how to specify the mlag peers to sync MAC entries on overlay logic ports:

Switch# configure terminal
Switch(config)# mlag configuration
Switch(config-mlag)# sync-overlay
Switch(config-mlag)#

Related Commands
show mlag

3.15.8 mlag

Command Purpose
The mlag command assigns an MLAG ID to a port-channel.

The no mlag command removes the MLAG ID assignment from the configuration mode interface by deleting the corresponding mlag command from running-config.

Command Syntax
mlag MLAGID
no mlag

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLAGID</td>
<td>Number used as MLAG ID.</td>
<td>1-55</td>
</tr>
</tbody>
</table>

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 agg 1
Switch(config-if)# mlag 1
Related Commands
show mlag interface

3.15.9 clear mlag count

Command Purpose
The clear mlag count command clears mlag count information.

Command Syntax
clear mlag count

Command Mode
Privileged EXEC

Default
None

Usage
Use this command to clear mlag count information which can be displayed by show mlag peer command.

Examples
This example shows how to clear mlag count information and display information about the MLAG peer:

Switch# clear mlag count
Switch# show mlag peer
MLAG neighbor is 12112, MLAG version 1
MLAG state = Established, up for 000039
Last read 000015; 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

3.15.10 show mlag

Command Purpose
The show mlag command displays information about the MLAG configuration.

Command Syntax
show mlag

Command Mode
Privileged EXEC
Default

None

Usage

Use this command to display information about the MLAG configuration.

Examples

This example shows how to display information about the MLAG configuration:

```
Switch# show mlag
MLAG configuration
------------------
role       Master
local_sysid 001e080a6fca
remote Sysid 000000000000
mlag_sysid 001e080a6fca
local Syspri 0
remote Syspri 0
peernode 32768
peer conf No
reload-delay 300

Related Commands

mlag configuration

3.15.11 show mlag peer

Command Purpose

The show mlag peer command displays information about the MLAG peer.

Command Syntax

show mlag peer (vlan-if |)

```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-if</td>
<td>Vlan interface information</td>
<td>-</td>
</tr>
</tbody>
</table>

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
```
Related Commands

peer-address

3.15.12  show mlag interface

Command Purpose
The show mlag interface command displays information about the MLAG interface.

Command Syntax
show mlag interface (MLAGID)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLAGID</td>
<td>Number used as MLAG ID.</td>
<td>1-55</td>
</tr>
</tbody>
</table>

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
Chapter 4 IP Service Commands

4.1 ARP Commands

4.1.1 Arp

Command Purpose

To add a permanent entry in the Address Resolution Protocol (ARP) cache, use the arp command in global configuration mode.

To remove an entry from the ARP cache, use the no form of this command.

Command Syntax

```
arp (vrf VRF-NAME | ) IP-ADDRESS HARDWARE-ADDRESS
no arp (vrf VRF-NAME | ) IP-ADDRESS
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf VRF-NAME</td>
<td>Virtual Routing and Forwarding (VRF) instance. The vrf-name argument is the name of the VRF table</td>
<td>String with up to 15 characters</td>
</tr>
<tr>
<td>IP-ADDRESS</td>
<td>IP address in four-part dotted decimal format corresponding to the local data-link address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>HARDWARE-ADDRESS</td>
<td>Local data-link address (a 48-bit address)</td>
<td>MAC Address</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>Time (in seconds) that an ARP request delay to interface</td>
<td>0-3 seconds</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>Time (in seconds) that an entry remains in the ARP cache. &lt;1-2147483&gt;</td>
<td>1-2147483 seconds</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

3600 seconds (1 hour)

Usage

This command is ignored when issued on interfaces that do not use ARP. The show interface EXEC command displays the ARP timeout value. The value as seen in the following example from the show interface command:

ARP timeout 01:00:00, ARP retry interval 1s

Examples

The following example sets the ARP timeout to 1200 seconds to allow entries to time out more quickly than the default:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# arp timeout 1200

Related Commands

show interface
4.1.4 arp as-layer-3 enable

Command Purpose

To set that deal with the arp packet as layer3 packet. To disable arp as-layer-3, use the no form of this command.

Command Syntax

arp as-layer-3 enable
no arp as-layer-3 enable

Command Mode

Global Configuration

Default

Disable

Usage

vlan classifier and IGMP Snooping affected by the CLI.

Enable, vlan classifier activate base ip, the arp packet matched source ip address will classifier to specified vlan. Otherwise, not classifier to specified vlan.

Enable, ip source guard enable the ip check on the port, the arp packet matched source ip address will not filter. Otherwise, will filter.

Examples

The following example show how to enable arp as-layer-3:

Switch# configure terminal
Switch(config)# arp as-layer-3 enable

Related Commands

N/A

4.1.5 arp fake global enable

Command Purpose

To enable fake arp global, use the no form of this command. To disable arp fake global, use the no form of this command.
Command Syntax

arp fake global enable
no arp fake global enable

Command Mode

Global Configuration

Default
Disable

Usage

Not effect until both enable global and interface arp fake.

Examples

The following example show how to enable global fake arp:

Switch# configure terminal
Switch(config)# arp fake global enable

Related Commands

arp fake enable

4.1.6  arp fake enable

Command Purpose

To enable fake arp on interface, use the no form of this command.

Command Syntax

arp fake enable
no arp fake enable

Command Mode

Interface Configuration

Default
Enable
Usage

If enable, the interface receive IP packets that not match any ARP entry will create an fake ARP entry. Before interface received ARP reply, the IP packets matched the fake ARP entry will be dropped. After interface received ARP reply, will create active ARP entry instead of fake ARP entry.

Examples

The following example show how to enable fake arp:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# arp fake enable

Related Commands

arp fake global enable

4.1.7 arp fake timeout

Command Purpose

To configure how long a fake entry remains in the ARP cache, use the arp fake timeout command in interface configuration mode. To restore the default value, use the no form of this command.

Command Syntax

arp fake timeout SECONDS
no arp fake timeout

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>Time that a fake entry remains in the ARP cache.</td>
<td>1-36000, unit: second</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

5 seconds

Usage

When switch was attached, can let the fake ARP entry to time out later.
Examples

The following example sets the ARP fake timeout to 100 seconds to allow entries to time out:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# arp fake timeout 100

Related Commands

N/A

4.1.8 clear arp-cache

Command Purpose

To refresh dynamically created entries from the Address Resolution Protocol (ARP) cache, use the clear arp-cache command in privileged EXEC mode.

Command Syntax

clear arp-cache ( ( vrf VRF-NAME | ) interface IFNAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf VRF-NAME</td>
<td>(Optional) Refreshes only the ARP table entries for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance</td>
<td>String with up to 15 characters</td>
</tr>
<tr>
<td>IFNAME</td>
<td>(Optional) Refreshes only the ARP table entries associated with this interface</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

No default behavior or values.

Usage

This command updates the dynamically learned IP address and MAC address mapping information in the ARP table to ensure the validity of those entries. If the refresh operation encounters any stale entries (dynamic ARP entries that have expired but have not yet been aged out by an internal, timer-driven process), those entries are aged out of the ARP table immediately as opposed to at the next refresh interval.

Use this command without any arguments or keywords to refresh all ARP cache entries for all enabled interfaces.
Examples

The following example shows how to refresh all dynamically learned ARP cache entries for all enabled interfaces:

Switch# clear arp-cache

Related Commands

show ip arp

4.1.9 clear ip arp

Command Purpose

To refresh the specific dynamically created entry from the Address Resolution Protocol (ARP) cache, use the clear ip arp command in privileged EXEC mode.

Command Syntax

clear ip arp (vrf VRF-NAME |) IP-ADDRESS

+----------------+---------------------------------+------------------+
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf VRF-NAME</td>
<td>(Optional) Refreshes only the ARP table entries for</td>
<td>String with up to 15 characters</td>
</tr>
<tr>
<td></td>
<td>the specified Virtual Private Network (VPN) routing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>and forwarding (VRF) instance</td>
<td></td>
</tr>
<tr>
<td>IP-ADDRESS</td>
<td>(Optional) Refreshes only the ARP table entries</td>
<td></td>
</tr>
<tr>
<td></td>
<td>associated with this IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

No default behavior or values.

Usage

This command updates the specific dynamically learned IP address and MAC address mapping information in the ARP table. If the refresh operation encounters any stale entries (dynamic ARP entries that have expired but have not yet been aged out by an internal, timer-driven process), the entry is aged out of the ARP table immediately as opposed to at the next refresh interval.

Examples

The following example shows how to refresh the dynamically learned ARP entries 10.10.10.10:

Switch# clear ip arp 10.10.10.10

Related Commands

show ip arp
4.1.10 clear ip arp statistics

Command Purpose

To clear ARP packets statistics processed by system, use the clear ip arp statistics command in privileged EXEC mode.

Command Syntax

```
clear ip arp (vrf VRF-NAME) statistics
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf VRF-NAME</td>
<td>(Optional) Clear ARP statistics for the specified</td>
<td>String with up to 15 characters</td>
</tr>
<tr>
<td></td>
<td>Virtual Private Network (VPN) routing and forwarding (VRF)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>instance</td>
<td></td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

No default behavior or values.

Usage

This command use to clear ARP packets statistics.

Examples

The following example shows how to clear ARP packets statistics:

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

Related Commands

show ip arp summary

4.1.11 show ip arp

Command Purpose

To display the entries in the Address Resolution Protocol (ARP) table, use the show ip arp command in privileged EXEC mode.
Command Syntax

`show ip arp { ( vrf VRF-NAME | ) interface INTERFACE-NAME | }`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf VRF-NAME</td>
<td>(Optional) Displays the entries under the Virtual Private Network (VPN) routing and</td>
<td>String with up to 15</td>
</tr>
<tr>
<td></td>
<td>forwarding (VRF) instance specified by the vrf-name argument</td>
<td>characters</td>
</tr>
<tr>
<td>INTERFACE-NAME</td>
<td>(Optional) Refreshes only the ARP table entries associated with this interface</td>
<td>-</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Address</th>
<th>Age (min)</th>
<th>Hardware Addr</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet</td>
<td>1.1.1.1</td>
<td>-</td>
<td>7cb5.0157.0c00</td>
<td>eth-0-1</td>
</tr>
<tr>
<td>Internet</td>
<td>2.2.2.1</td>
<td>-</td>
<td>7cb5.0157.0c00</td>
<td>eth-0-2</td>
</tr>
<tr>
<td>Internet</td>
<td>3.3.3.1</td>
<td>-</td>
<td>7cb5.0157.0c00</td>
<td>eth-0-3</td>
</tr>
<tr>
<td>Internet</td>
<td>10.0.20.1</td>
<td>-</td>
<td>7cb5.0157.0c00</td>
<td>eth-0-10</td>
</tr>
<tr>
<td>Internet</td>
<td>10.0.20.254</td>
<td>-</td>
<td>0000.5e00.0101</td>
<td>eth-0-10</td>
</tr>
</tbody>
</table>
```

Related Commands

- `clear ip arp`

4.1.12 `show ip arp summary`

Command Purpose

To display the total number of Address Resolution Protocol (ARP) table entries, the number of ARP table entries for each ARP entry mode, and the number of ARP table entries for each interface on the router, use the `show ip arp summary` command in privileged EXEC mode.
Command Syntax

show ip arp (vrf VRF-NAME | summary

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf VRF-NAME</td>
<td>(Optional) Displays the entries under the Virtual</td>
<td>String with up to 15 characters</td>
</tr>
<tr>
<td></td>
<td>Private Network (VPN) routing and forwarding</td>
<td>(VRF) instance specified by the vrf-name argument</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to display high-level statistics about the ARP table entries:

Examples

The following is sample output from the show ip arp summary command:

Switch# show ip arp summary

Gratuitous ARP learning is disabled
2 IP ARP entries, with 0 of them incomplete
(Static:1, Dynamic:0, Interface:1)
ARP Pkt Received is: 0
ARP Pkt Send number is: 1
ARP Pkt Dicard number is: 0

Related Commands

clear ip arp statistics

4.1.13 debug arp

Command Purpose

To turn on the ARP debug, use debugs arp command in EXEC mode. To turn off the ARP debug, use the no form of this command.

Command Syntax

default arp (vrf VRF-NAME |)
The following is sample output from the `debug arp` command:

```
Switch# debug arp
Sep 7 03:34:08 SWITCH ARP-7: IP ARP: creating entry for IP address: 7.7.7.7, hw: e64d.0445.df00
Sep 7 03:34:08 SWITCH ARP-7: IP ARP: send req src 7.7.7.7 e64d.0445.df00, dst 7.7.7.7 eth-0-1
```

**Related Commands**

- `show debugging arp`
- `4.1.14 show debugging arp`

**Command Purpose**

To display the debugging status of ARP, use the `show debugging arp` command in EXEC mode.

**Command Syntax**

```
show debugging arp (vrf VRF-NAME | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vrf VRF-NAME</code></td>
<td>(Optional) Displays the entries under the Virtual Private Network (VPN) routing and forwarding (VRF) instance specified by the vrf-name argument</td>
<td>String with up to 15 characters</td>
</tr>
</tbody>
</table>
Command Mode
Privileged EXEC

Default
None

Usage

Use this command to display the debugging status of ARP.

Examples

The following is sample output from the show debugging arp command:

```
Switch# show debugging arp
ARP debugging status:
  ARP packet debugging is on
```

Related Commands
debug arp

4.1.15 proxy-arp enable

Command Purpose

The switch uses proxy ARP to help hosts determine MAC addresses of hosts on other networks or subnets.

To enable proxy Address Resolution Protocol (ARP) on an interface, use the proxy-arp enable command in interface configuration mode.

To disable proxy ARP on the interface, use the no form of this command.

Command Syntax

proxy-arp enable

Command Mode

Interface Configuration

Default

Proxy ARP is disabled by default.
Usage

When proxy ARP is disabled, a device will respond to ARP requests received on its interface only if the target IP address is the same as its IP address.

Examples

The following example enables proxy ARP on interface eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 1.1.1.1/24
Switch(config-if)# proxy-arp enable
```

Related Commands

local-proxy-arp enable

4.1.16 local-proxy-arp enable

Command Purpose

The local proxy ARP feature allow the L3 Device to response ARP request whose ARP Target address is in the same subnet the as the ARP request comes from (No Routing is required).

To enable local proxy Address Resolution Protocol (ARP) on an interface, use the local-proxy-arp enable command in interface configuration mode.

To disable proxy ARP on the interface, use the no form of this command.

Command Syntax

local-proxy-arp enable

no local-proxy-arp enable

Command Mode

Interface Configuration

Default

Local proxy ARP is disabled by default.

Usage

Internet Control Message Protocol (ICMP) redirects are disabled on interfaces when the local proxy ARP feature is enabled. The main condition we need to enable local ARP proxy is that the switch enables port isolate.
Examples
The following example enables local proxy ARP on interface eth-0-1:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 1.1.1.1/24
Switch(config-if)# local-proxy-arp enable

Related Commands
proxy-arp enable

4.1.17 gratuitous-arp-learning enable

Command Purpose
To enable the gratuitous Address Resolution Protocol (ARP) control on the router, use the gratuitous-arp-learning enable command in global configuration mode. To disable the ARP control, use the no form of this command.

Command Syntax
gratuitous-arp-learning enable
no gratuitous-arp-learning enable

Command Mode
Global Configuration

Default
Gratuitous ARP learning is disabled by default.

Usage
None

Examples
The following example enables gratuitous ARP learning on interface eth-0-1:

Switch# configure terminal
Switch(config)# gratuitous-arp-learning enable

Related Commands
show ip arp summary

4.1.18 gratuitous-arp send interval

Command Purpose
To config the gratuitous ARP send interval, use the no form of this command to recover to default.
Command Syntax

```
arp gratuitous-arp send interval SECONDS

no arp gratuitous-arp send interval
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>The interval in seconds to send gratuitous ARP</td>
<td>1-86400 seconds</td>
</tr>
</tbody>
</table>

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

4.1.19  gratuitous-arp send enable
```

Command Purpose

To enable the gratuitous ARP send on the interface.

Command Syntax

```
arp gratuitous-arp send enable

no arp gratuitous-arp send enable
```
Command Mode

Interface Configuration

Default

Disable

Usage

None

Examples

The following example enable gratuitous ARP on interface eth-0-1:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 1.1.1.1/24
Switch(config-if)# arp gratuitous-arp send enable

Related Commands

arp gratuitous-arp send interval

4.2 DHCP Client Commands

4.2.1 ip address dhcp

Command Purpose

To acquire an IP address from Dynamic Host Configuration Protocol(DHCP), use the ip address dhcp command in interface configuration mode.
To disable the function, use the no form of this command.

Command Syntax

ip address dhcp

no ip address dhcp
Command Mode

Interface Configuration

Default

DHCP Client is not enabled on interface.

Usage

Once this command was enabled on an UP interface, it will acquire IP address immediately, otherwise the DHCP function of the interface will be in SUSPEND status.

The no ip address dhcp command will send a DHCPRELEASE message to server and remove any IP address.

Examples

The following example shows how to enable dhcp client function:

Switch# configure terminal
Switch(config-if)# ip address dhcp

The following example shows how to disable dhcp client function:

Switch# configure terminal
Switch(config-if)# no ip address dhcp

Related Commands

dhcp client request
dhcp client client-id
dhcp client class-id
dhcp client lease
dhcp client hostname
management ip address dhcp
show dhcp client

4.2.2 management ip address dhcp

Command Purpose

To acquire an IP address for management interface from by DHCP, use the management IP address dhcp command in global configuration mode.

To disable the function, use the no form of this command.

Command Syntax

management ip address dhcp
no management ip address dhcp

**Command Mode**

Global Configuration

**Default**

DHCP Client is not enabled on management interface.

**Usage**

Use this command like IP address dhcp.

**Examples**

The following example shows how to enable dhcp client function on management interface:

```
Switch# configure terminal
Switch(config)# management ip address dhcp
```

The following example shows how to disable dhcp client function on management interface:

```
Switch# configure terminal
Switch(config)# no management ip address dhcp
```

**Related Commands**

show dhcp client

**4.2.3 dhcp client request**

**Command Purpose**

To request configuration parameters by DHCP, use the dhcp client request command in interface configuration mode. To cancel the request, use the no form of this command.

**Command Syntax**

```
dhcp client request ( router | static-route | classless-static-route | classless-static-route-ms | tftp-server-address | dns-nameserver | domain-name | netbios-nameserver | vendor-specific )
```

```
no dhcp client request ( router | static-route | classless-static-route | classless-static-route-ms | tftp-server-address | dns-nameserver | domain-name | netbios-nameserver | vendor-specific )
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>router</td>
<td>Default router option (3)</td>
<td>-</td>
</tr>
<tr>
<td>static-route</td>
<td>Static route option (33)</td>
<td>-</td>
</tr>
<tr>
<td>classless-static-route</td>
<td>Classless static route option (121)</td>
<td>-</td>
</tr>
<tr>
<td>classless-static-route-ms</td>
<td>Microsoft classless static route option (249)</td>
<td>-</td>
</tr>
<tr>
<td>tftp-server-address</td>
<td>TFTP server ip address option (150)</td>
<td>-</td>
</tr>
<tr>
<td>dns-nameserver</td>
<td>DNS name server option (6)</td>
<td>-</td>
</tr>
<tr>
<td>domain-name</td>
<td>Domain name option (15)</td>
<td>-</td>
</tr>
<tr>
<td>netbios-nameserver</td>
<td>NetBIOS name server option (44)</td>
<td>-</td>
</tr>
<tr>
<td>vendor-specific</td>
<td>Vendor specific option (43)</td>
<td>-</td>
</tr>
</tbody>
</table>

**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 )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ascii</td>
<td>ASCII type</td>
<td>-</td>
</tr>
<tr>
<td>WORD</td>
<td>Client-ID as ascii string</td>
<td>String with up to 64 characters</td>
</tr>
<tr>
<td>hex</td>
<td>Hex type</td>
<td>-</td>
</tr>
<tr>
<td>HEX-STRING</td>
<td>Class-ID in hex string</td>
<td>String with up to 64 characters</td>
</tr>
<tr>
<td>IFVLAN</td>
<td>Vlan interface's name</td>
<td>1-4094</td>
</tr>
<tr>
<td>IFAGG</td>
<td>Aggregation interface's name</td>
<td>-</td>
</tr>
<tr>
<td>IFPHYSICAL</td>
<td>Physical interface's name</td>
<td>-</td>
</tr>
</tbody>
</table>

**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)# 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>Client-ID as ascii string</td>
<td>-</td>
</tr>
<tr>
<td>hex</td>
<td>Hex type</td>
<td>-</td>
</tr>
<tr>
<td>HEX-STRING</td>
<td>Class-ID in hex string</td>
<td>-</td>
</tr>
</tbody>
</table>

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:

```plaintext
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dhcp client class-id ascii switch
```

The following example shows how to delete class-id set before:

```plaintext
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DAYS</td>
<td>The number of days in lease</td>
<td>0-365</td>
</tr>
<tr>
<td>HOURS</td>
<td>The number of hours in the lease.</td>
<td>0-23</td>
</tr>
<tr>
<td>MINUTES</td>
<td>The number of minutes in the lease</td>
<td>0-59</td>
</tr>
<tr>
<td>infinite</td>
<td>infinite lease</td>
<td>-</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>Host name</td>
<td>String with up to 256 characters</td>
</tr>
</tbody>
</table>

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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>METRIC</td>
<td>The default metric of routes</td>
<td>1-255</td>
</tr>
</tbody>
</table>

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 tells 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 }
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>events</td>
<td>Client events</td>
<td>-</td>
</tr>
<tr>
<td>error</td>
<td>Error DHCP message</td>
<td>-</td>
</tr>
<tr>
<td>packet</td>
<td>DHCP message fields</td>
<td>-</td>
</tr>
<tr>
<td>dump</td>
<td>Dump message in hex format</td>
<td>-</td>
</tr>
<tr>
<td>all</td>
<td>Turn all debugging on</td>
<td>-</td>
</tr>
</tbody>
</table>

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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>management</td>
<td>Management interface</td>
<td>-</td>
</tr>
<tr>
<td>IFVLAN</td>
<td>Vlan interface's name</td>
<td>1-4094</td>
</tr>
<tr>
<td>IFAGG</td>
<td>Aggregation interface's name</td>
<td>-</td>
</tr>
<tr>
<td>IFPHYSICAL</td>
<td>Physical interface's name</td>
<td>-</td>
</tr>
<tr>
<td>verbose</td>
<td>DHCP client verbose information</td>
<td>-</td>
</tr>
</tbody>
</table>

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 | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>Number of the DHCP server group.</td>
<td>1-16</td>
</tr>
<tr>
<td>SERVER-LIST</td>
<td>The IP address list of the DHCP server.</td>
<td>1-16</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>Number of the DHCP server group.</td>
<td>1-16</td>
</tr>
</tbody>
</table>

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 Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>drop</strong></td>
<td>Directs the DHCP relay agent to discard messages with existing relay information if the relay information option is already present.</td>
<td>-</td>
</tr>
<tr>
<td><strong>keep</strong></td>
<td>Indicates that existing information is left unchanged on the DHCP relay agent.</td>
<td>-</td>
</tr>
<tr>
<td><strong>replace</strong></td>
<td>Indicates that existing information is overwritten on the DHCP relay agent.</td>
<td>-</td>
</tr>
</tbody>
</table>

#### 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 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

4.3.8 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

4.3.9 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)

4.3.10  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
4.3.11 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
4.3.12 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

download dhcp relay (events | error | dump | packet | all)

no download dhcp relay (events | error | dump | packet | all)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>events</td>
<td>Relay events</td>
<td></td>
</tr>
<tr>
<td>error</td>
<td>Error DHCP message</td>
<td></td>
</tr>
<tr>
<td>packet</td>
<td>DHCP message fields</td>
<td></td>
</tr>
<tr>
<td>dump</td>
<td>Dump message in hex format</td>
<td></td>
</tr>
<tr>
<td>all</td>
<td>Turn all debugging on</td>
<td></td>
</tr>
</tbody>
</table>

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

4.3.13 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)

**4.3.14 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

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>DHCP server group</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-0-1</td>
<td>1</td>
</tr>
</tbody>
</table>

Related Commands

show dhcp-server

4.3.15  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

4.3.16 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

4.3.17 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

### 4.3.18 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Specify a L3 interface to act as a DHCP server</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>Remove DHCP server on a L3 interface</td>
<td>-</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>Specify the number of ping packets that are sent before assigning the address to a requesting client</td>
<td>0-10</td>
</tr>
</tbody>
</table>
**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>Specifies how long to wait for a ping reply in seconds.</td>
<td>1-10 seconds</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>WORD: The name of a DHCP pool</td>
<td>1) the length range should be [1, 32] 2) The characters can only include [0-9a-zA-Z-_] 3) The string must start with alphabetic, ending with alphanumeric or digit</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>IP address.</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IP_ADDR_MASK</td>
<td>IP-address-type mask</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IP_MASK_LEN</td>
<td>Prefix length for the ip address.</td>
<td>1-32</td>
</tr>
<tr>
<td>mac-address</td>
<td>the hardware address of a DHCP client.</td>
<td>MAC Address</td>
</tr>
<tr>
<td>MAC_ADDR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ascii WORD</td>
<td>the client id as ascii string</td>
<td>String with up to 63 characters</td>
</tr>
<tr>
<td>hex HEX_STRING</td>
<td>the client id as hex string</td>
<td>String with up to 126 characters</td>
</tr>
</tbody>
</table>
**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

<table>
<thead>
<tr>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>A.B.C.D… A.B.C.D (Optional)</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td></td>
<td>Specifies up to eight addresses in the command line.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
</table>
| WORD      | specify a domain 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 alphanumerical or digit |
Command Mode

DHCP pool Configuration

Default

The default value is none domain-name specified.

Usage

You can specify a domain name suffix in each DHCP address pool on the DHCP server for the clients. With this suffix assigned, the client needs only input part of a domain name, 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
</table>
| 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D</td>
<td>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.</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>A.B.C.D... A.B.C.D (Optional)</td>
<td>Specifies up to eight address in the command line.</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>
**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D</td>
<td>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.</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>A.B.C.D... A.B.C.D (Optional)</td>
<td>Specifies up to eight addresses in the command line.</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>
**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)
nob netbios-name-server
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D</td>
<td>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.</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>A.B.C.D... A.B.C.D (Optional)</td>
<td>Specifies up to eight addresses in the command line.</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>
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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>b-node</td>
<td>Broadcast</td>
<td>-</td>
</tr>
<tr>
<td>p-node</td>
<td>Peer-to-peer</td>
<td>-</td>
</tr>
<tr>
<td>m-node</td>
<td>Mixed</td>
<td>-</td>
</tr>
<tr>
<td>h-node</td>
<td>Hybrid (recommended)</td>
<td>-</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address.</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>wildcard-mask</td>
<td>IP-address-type mask that includes &quot;don't care&quot; bits.</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>prefix-length</td>
<td>Prefix length for the network.</td>
<td>0-32</td>
</tr>
</tbody>
</table>

Command Mode

DHCP pool Configuration
Default

The default value is none subnet number and mask specified.

Usage

This command is valid for DHCP subnetwork address pools only. The DHCP server assumes that all host addresses are available. The system administrator can exclude subsets of the address space by using the `ip dhcp excluded-address` command. Network for one pool can’t 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 | |))
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DAYS</td>
<td>Specifies the duration of the lease in numbers of days.</td>
<td>0-365 days</td>
</tr>
<tr>
<td>HOURS (Optional)</td>
<td>Specifies the number of hours in the lease. A day's value must be supplied before you can configure an hour's value.</td>
<td>0-23 hours</td>
</tr>
<tr>
<td>MINUTES (Optional)</td>
<td>Specifies the number of minutes in the lease. A day's value and an hour value must be supplied before you can configure a minute's value.</td>
<td>0-59 minutes</td>
</tr>
</tbody>
</table>
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 ]
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>code</td>
<td>Specifies the DHCP option code.</td>
<td>2-254</td>
</tr>
<tr>
<td>ascii-string</td>
<td>Specifies an NVT ASCII character string. ASCII character strings that contain white space must be delaminated by quotation marks.</td>
<td>String with up to 63 characters</td>
</tr>
<tr>
<td>hex-string</td>
<td>Specifies dotted-hexadecimal data. Each byte in hexadecimal character strings is two hexadecimal digits.</td>
<td>String with up to 126 characters</td>
</tr>
<tr>
<td>ip-address</td>
<td>Specifies an IP address.</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

**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 Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D</td>
<td>The excluded IP address, or low IP address in an excluded address range.</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>A.B.C.D(Optional)</td>
<td>The high IP address in the excluded address range.</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

### 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 ]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip A.B.C.D</td>
<td>Specifies the IP address of the conflict found.</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all IP address of the conflict found.</td>
<td>-</td>
</tr>
</tbody>
</table>
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 ]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip A.B.C.D</td>
<td>Specifies the IP address of the conflict found.</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>pool WORD</td>
<td>Specifies the pool name where the IP address of the conflict found.</td>
<td>String with up to 31 characters</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all conflict IP address.</td>
<td>-</td>
</tr>
</tbody>
</table>

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 ]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip A.B.C.D</td>
<td>The IP address of the host that contains the conflicting address you want to clear.</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>all</td>
<td>Clear all conflicting address.</td>
<td>-</td>
</tr>
</tbody>
</table>

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 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 ]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip A.B.C.D</td>
<td>The address of the binding you want to clear.</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>pool WORD</td>
<td>Specifies the pool name where the IP address of the conflict found.</td>
<td>String with up to 31 characters</td>
</tr>
<tr>
<td>all</td>
<td>Clears all automatic bindings.</td>
<td>-</td>
</tr>
</tbody>
</table>

**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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>Specifies the pool name to display pool utilization.</td>
<td>String with up to 31 characters</td>
</tr>
</tbody>
</table>

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
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool</td>
<td>pool1</td>
</tr>
<tr>
<td>Type</td>
<td>Dynamic</td>
</tr>
<tr>
<td>Lease</td>
<td>0 Days 0 Hours 5 Minutes</td>
</tr>
<tr>
<td>Total addresses</td>
<td>254</td>
</tr>
<tr>
<td>Leased addresses</td>
<td>1</td>
</tr>
<tr>
<td>Excluded addresses</td>
<td>1</td>
</tr>
<tr>
<td>Free addresses</td>
<td>252</td>
</tr>
<tr>
<td>Conflict addresses</td>
<td>0</td>
</tr>
<tr>
<td>Current index IP address range</td>
<td>Leased/Excluded/Total</td>
</tr>
<tr>
<td>2.1.1.5</td>
<td>2.1.1.1 - 2.1.1.254</td>
</tr>
</tbody>
</table>

Related Commands

4.5 DNS Commands

4.5.1 ip host

Command Purpose

To define static hostname-to-address mappings in the Domain Name System (DNS) hostname cache for a DNS view, use the `ip host` command in global configuration mode. If the hostname cache does not exist yet, it is automatically created.

To remove a hostname-to-address mapping, use the `no` form of this command.

Command Syntax

```
ip host HOSTNAME IP_ADDR

no ip host hostname
```
### 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
```

**Table:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOSTNAME</td>
<td>Name of the host</td>
<td>String with up to 63 characters</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>Associated host IP address</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPADDR</td>
<td>IP address of a DNS name server</td>
<td>Support IPv4/IPv6 Address</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Name of source interface</td>
<td>Support physical/aggregation/loopback/tunnel/vlan ports</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Source IP address</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

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 }
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain</td>
<td>Display DNS domain list</td>
<td>-</td>
</tr>
<tr>
<td>server</td>
<td>Display DNS server list</td>
<td>-</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Suffix</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>domain</td>
</tr>
<tr>
<td>2</td>
<td>aa.com</td>
</tr>
</tbody>
</table>

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 Mod
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:

<table>
<thead>
<tr>
<th>Host</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.sampledomain.com">www.sampledomain.com</a></td>
<td>1.1.1.1</td>
</tr>
</tbody>
</table>

Related Commands
ip host
Chapter 5 IPv6 Service Commands

5.1 Tunnel Commands

5.1.1 interface

Command Purpose

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TUNNEL-ID</td>
<td>The tunnel id</td>
<td>0-1023</td>
</tr>
</tbody>
</table>

Command Syntax

interface tunnel TUNNEL-ID
no interface tunnel TUNNEL-ID

Command Mode

Global Configuration

Default
None

Usage

Before connect 2 IPv6 networks by an IPv4 network, a tunnel interface is required. The tunnel is available after set some attributes. After IPv6 is enabled the tunnel interface can forward IPv6 packets.

Examples

This example shows how to create a tunnel interface:

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

Related Commands

show interface tunnel

5.1.2 tunnel mode

Command Purpose

Use this command to specify the IPv6 transition tunnel protocol. Use the no form of this command to unset the tunnel protocol.

Command Syntax

tunnel mode tunnel mode ( erspan ( ecmp-dst-gre ) | gre | ipv6ip ) ( 6to4 | isatap )
no tunnel mode
Command Mode

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>6to4</td>
<td>Set the tunnel as automatic tunnel 6to4, which use 2002::/16 as its prefix</td>
<td>-</td>
</tr>
<tr>
<td>isatap</td>
<td>Set the tunnel as automatic tunnel ISATAP, which use :::fe:a:b.c.d as its suffix</td>
<td>-</td>
</tr>
<tr>
<td>gre</td>
<td>When the destination of tunnel is single, the mode of the tunnel</td>
<td>-</td>
</tr>
<tr>
<td>ecmp-dst-gre</td>
<td>When the destinations of tunnel are multi, the mode of the tunnel</td>
<td>-</td>
</tr>
</tbody>
</table>

Interface Configuration

**Default**

None

**Usage**

This command specifies a tunnel encapsulation mode for IPv6 in IPv4. When the keywords "6to4" or "isatap" is not specified, then it is a manual tunnel. Tunnel mode is not allowed to change from 6to4 to ISATAP when 6to4 relay routes are configured. Users should unset the tunnel destination before change from manual tunnel to automatic tunnel.

**Examples**

This example shows how to create a 6to4 Tunnel:

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel mode ipv6ip 6to4
```

**Related Commands**

tunnel source

tunnel destination

### 5.1.3 tunnel source

**Command Purpose**

Use this command to specify the tunnel source. Use the no form of this command to unset the tunnel source.

**Command Syntax**

```
tunnel source (IP_ADDR | IFNAME)
```

no tunnel source

**Command Mode**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>Specify a tunnel source in the IPv4 address format</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Specify a tunnel source in the IFNAME format, the IFNAME should be layer3 interface</td>
<td>Supportphysical/aggregation/loopback/vlan/ports</td>
</tr>
</tbody>
</table>

Interface Configuration

**Default**

None

Every tunnel must have a tunnel source. If users specify the IFNAME format, system will choose the primary address as tunnel source.
Examples

This example shows how to set the tunnel source:

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel source 3.3.3.3
```

Related Commands

```
tunnel mode ipv6ip
tunnel destination
```

5.1.4 tunnel destination

Command Purpose

Use this command to specify a tunnel destination address in an IPv4 portion. Use the no parameter to un-specify the address.

Command Syntax

```
tunnel destination IP_ADDR
no tunnel destination
```

Command Mode

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>Specify the tunnel destination IPv4 address</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

Interface Configuration

Default

None

Usage

Automatic tunnel such as 6to4 and ISATAP must not configure tunnel destination.

Examples

This example shows how to set the tunnel destination:

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel destination 4.4.4.4
```

Related Commands

```
tunnel source
tunnel mode ipv6ip
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enable tunnel decapsulation</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>Disable tunnel decapsulation</td>
<td>-</td>
</tr>
</tbody>
</table>
5.1.5 tunnel enable

Command Purpose
Use this command to enable tunnel decapsulation for interfaces. Use the form of this command to restore the default configuration.

Command Syntax
```
tunnel ( enable | disable )
```

Command Mode
Interface Configuration

Default
By default, tunnel decapsulation is disabled on all interfaces.

Usage
None

Examples
This example shows how to enable tunnel decapsulation on interface eth-0-1:
```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# tunnel enable
```

Related Commands
Interface

5.1.6 tunnel ecmp-destination

Command Purpose
Use this command to configure tunnel ECMP destinations IP address. Use the form of this command to unset this configuration.

Command Syntax
```
tunnel ecmp-destination IP_ADDR
no tunnel ecmp-destination IP_ADDR
```

Command Mode

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>ECMPdestinations IP address</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

Interface Configuration

Default
None

Usage
Automatic tunnel such as 6to4 and ISATAP must not configure tunnel destination (multi destination).
Examples

This example shows how to enable tunnel decapsulation on interface tunnel 1:
```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel ecmp-destination 1.1.1.1
Switch(config-if)# tunnel ecmp-destination 2.2.2.2
```

Related Commands

tunnel source
tunnel mode (ecmp-dst-gre | ) | gre)

5.1.7 tunnel gre key

Command Purpose

Use this command to configure the tunnel gre key value.
Use the form of this command to unset this configuration

Command Syntax

```
tunnel gre key KEY_VALUE
no tunnel gre key
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEY_VALUE</td>
<td>gre key value</td>
<td>1-4294967295</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

None

Usage

Improve the security of the gre tunnel, configure the gre key to do the checkout of point to point.

Examples

This example shows how to enable tunnel decapsulation on interface tunnel 1:
```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel gre key 100
```

Related Commands

show running-config interface tunnel

5.1.8 tunnel extend-header

Command Purpose

Before the mirror traffic passes through the tunnel, encapsulate the traffic with the extend header.
Use no the form of this command to unset this configuration.

Command Syntax

```
tunnel extend-header
no tunnel extend-header
```

Command Mode

Interface Configuration
Default
None

Usage
- spanExtendHeaderCopyHash, using the new hash or not;
- PacketInfo.skipTimInfoUpdate, fixed with 1;
- if spanExtendHeaderCopyHash is 1, the filed consist with hash (8 bit) and 0 (8 bit); if spanExtendHeaderCopyHash is 0, the filed consist with source port of the mirror (16 bit).
Without dst-load-balance parameter, spanExtendHeaderCopyHash will be 0, and extend-header field does not contain the hash value; with dst-load-balance parameter, spanExtendHeaderCopyHash will be 1, and extend-header field contain the hash value.

Examples
This example shows how to enable extend-header hash for load balance:
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel extend-header dst-load-balance

Related Commands
show running-config interface tunnel

5.1.9 tunnel extend-header id

Command Purpose
Use this command to configure the extend header id.
Use the no form of this command to unset this configuration.

Command Syntax
tunnel extend-header id ID_VALUE

Parameter | Parameter Description | Parameter Value
---|---|---
ID_VALUE | The extend header id value | 1-1023

extend-header id ID_VALUE

Command Mode
Interface Configuration

Default
0

Usage
None

Examples
This example shows how to enable tunnel decapsulation on interface tunnel 1:
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel extend-header id 30

Related Commands
show running-config interface tunnel
5.1.10 tunnel dscp

Command Purpose

Use this command to specify a value of Differentiated Services Code Point (DSCP) in the tunnel IPv4 encapsulation header. Use the no parameter to inheriting the underlying physical interface value by default.

Command Syntax

tunnel dscp DSCP
no tunnel dscp

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP</td>
<td>The outer IPv4 header DSCP value</td>
<td>0-63</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

By default, the DSCP value is inherited from original IPv6 packet.

Usage

None

Examples

This example shows how to set the outer IPv4 header DSCP value as 40:

Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel dscp 40

Related Commands

Interface

5.1.11 tunnel ttl

Command Purpose

Use this command to specify a value of time to live (TTL) in the tunnel IPv4 encapsulation header. Use the no parameter to inheriting the underlying physical interface value by default.

Command Syntax

tunnel ttl TTL
no tunnel TTL

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TTL</td>
<td>The outer IPv4 header TTL value</td>
<td>1-254</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

By default, the TTL value is inherited from original IPv6 packet.

Usage

None
Examples

This example shows how to set the outer IPv4 header TTL value as 254:
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel ttl 254

Related Commands

Interface

5.1.12  ipv6 mtu

Command Purpose

Use this command to specify the Tunnel interface MTU.
Use the no form of this command to restore to the default value.

Command Syntax

ipv6 mtu MTU
no ipv6 mtu

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTU</td>
<td>Set the tunnel interface MTU</td>
<td>1280-9500</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

1480

Usage

System does not support Path MTU Discovery on tunnel interface. This command is only allowed on tunnel interface.

Examples

This example sets the tunnel interface MTU to 1280:
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# ipv6 mtu 1280

Related Commands

tunnel ttl

5.1.13  show interface tunnel

Command Purpose

Use this command to display the tunnel information.

Command Syntax

show interface tunnel TUNNEL-ID

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TUNNEL-ID</td>
<td>The tunnel id</td>
<td>0-1023</td>
</tr>
</tbody>
</table>
Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example displays the tunnel information:
Switch# show interface tunnel1

<table>
<thead>
<tr>
<th>Interface tunnel1</th>
<th>Interface current state: UP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware is Tunnel</td>
<td></td>
</tr>
<tr>
<td>Index 8193, Metric 1, Encapsulation TUNNEL</td>
<td></td>
</tr>
<tr>
<td>VF binding: not bound</td>
<td></td>
</tr>
<tr>
<td>Tunnel protocol/transport IPv6/IP, Status Valid</td>
<td></td>
</tr>
<tr>
<td>Tunnel source 1.1.1.1(eth-0-1), destination 2.2.2.2</td>
<td></td>
</tr>
<tr>
<td>Tunnel DSCP inherit, Tunnel TTL 64</td>
<td></td>
</tr>
<tr>
<td>Tunnel transport MTU 1480 bytes</td>
<td></td>
</tr>
</tbody>
</table>

Related Commands
show ipv6 interface tunnel

5.1.14 show resource tunnel

Command Purpose
Use this command to display the tunnel peers resource information.

Command Syntax
show resource tunnel

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example displays the tunnel peers resource information:
Switch# show resource tunnel

<table>
<thead>
<tr>
<th>Tunnel Resource</th>
<th>Used</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peers</td>
<td>1</td>
<td>8</td>
</tr>
</tbody>
</table>

Related Commands
None
5.2 NDP Commands

5.2.1 ipv6 neighbor

Command Purpose
Use this command to configure a static neighbor entry.
To delete the static neighbor entry, use the no form of this command.

Command Syntax
ipv6 neighbor (vrf NAME |) IPV6_ADDR MAC (IFNAME |)
no ipv6 neighbor (vrf NAME |) IPV6_ADDR (IFNAME |)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf NAME</td>
<td>vrf instance name</td>
<td>String with up to 15 characters</td>
</tr>
<tr>
<td>IPV6_ADDR</td>
<td>IPv6 address in X:X::X:X format</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>MAC</td>
<td>MAC address in HHHH.HHHH.HHHH format</td>
<td>MAC Address</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
By default, there is not any static ipv6 neighbor entry exist.

Usage
Use this command to configure a static neighbor entry. If the IPv6 address is link-local, the interface name must be specified. Using the no form of this command should not remove any dynamic neighbor entries.

Examples
This example shows how to add a static neighbor entry:
Switch# configure terminal
Switch(config)# ipv6 neighbor 2001::1 0000.0000.0001
Switch(config)# ipv6 neighbor vrf a fe80::1 0000.0000.0002 eth-0-1

Related Commands
show ipv6 neighbors

5.2.2 clear ipv6 neighbors

Command Purpose
Use this command to clear the dynamic neighbor entries.

Command Syntax
clear ipv6 neighbors (vrf NAME |) (interface IFNAME |)
Clearipv6 neighbors (vrf NAME |) IPV6_ADDR (interface IFNAME |)
### clear ipv6 neighbors

**Parameter**
- **vrf NAME**
  - vrf instance name: String with up to 15 characters
- **interface IFNAME**
  - Clear neighbor cache on the interface: Support physical/aggregation/loopback/vlan/tunnel ports
- **IPV6_ADDR**
  - IPv6 address in X::XX format. Clear IPv6 neighbor cache by address: IPv6 Address

**Command Mode**
- Privileged EXEC

**Default**
- None

**Usage**
Use this command to clear the dynamic neighbor entries. User can clear dynamic ipv6 address by interface or address. If the specified address is link-local, the interface is required.

**Examples**
This example shows how to clear the neighbor entries:
```
Switch# clear ipv6 neighbors
```

**Related Commands**
- show ipv6 neighbors

### ipv6 hop-limit

**Command Purpose**
Use this command to set the ipv6 hop limit of the packets. To restore the default configuration, use the no form of this command.

**Command Syntax**
- ipv6 hop-limit **HOP_LIMIT**
- no ipv6 hop-limit

**Parameter**
- **hop-limit HOP_LIMIT**
  - Hop limit: 1-255

**Command Mode**
- Global Configuration

**Default**
- By default, the value is 64.

**Usage**
The hop limit setting should affect all IPv6 packets send from this device, unless the hop-limit is overwritten by up layer application, for example, OSPF, etc.
Examples

This example shows how to set the hop limit:
Switch# configure terminal
Switch(config)# ipv6 hop-limit 255

Related Commands
None

5.2.4 ipv6 nd ra hop-limit

Command Purpose
Use this command to set the “Current hop limit” in RA packets.
To restore the default configuration, use the no form of this command.

Command Syntax
ipv6 nd ra hop-limit HOP_LIMIT
no ipv6 nd ra hop-limit

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>hop-limit HOP_LIMIT</td>
<td>Set cur hop limit.</td>
<td>0-255</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
By default, the value is 0.

Usage
None

Examples

This example shows how to set the “Current hop limit” in RA packets:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 nd ra hop-limit 255

Related Commands
None

5.2.5 ipv6 nd dad attempts

Command Purpose
Use this command to set the attempt times of DAD (Duplicate Address Detect).
To restore the default configuration, use the no form of this command.

Command Syntax
ipv6 nd dad attempts DAD_ATTEMPTS
no ipv6 nd dad attempts
Command Mode

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DAD_ATTEMPTS</td>
<td>Set attempts number.</td>
<td>0-600</td>
</tr>
</tbody>
</table>

Interface Configuration

Default

By default, the value is 1.

Usage

Use this command to set the attempt times of DAD (Duplicate Address Detect). "0" means DAD feature is disabled.

Examples

This example shows how to set the dad attempt:
```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 nd dad attempts 3
```

Related Commands

None

5.2.6 ipv6 nd ns-interval

Command Purpose

Use this command to set the interval of NS packets.
To restore the default configuration, use the no form of this command.

Command Syntax

```
ipv6 nd ns-interval NS_INTERVAL
no ipv6 nd ns-interval
```

Command Mode

Interface Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NS_INTERVAL</td>
<td>Set IPv6 neighbor solicitation interval.</td>
<td>1000-3600000 milliseconds</td>
</tr>
</tbody>
</table>

Default

By default, the value is 1000

Usage

This configuration should affect the interval of NS packet during the DAD period or neighbor discovery period.

Example

This example shows how to set the ns interval:
```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 nd ns-interval 2000
```
Related Commands

None

5.2.7 ipv6 nd ra suppress

Command Purpose

Use this command to enable the RA suppress function. To disable this function, use the no form of this command.

Command Syntax

ipv6 nd ra suppress
no ipv6 nd ra suppress

Command Mode

Interface Configuration

Default

By default, RA suppress is enabled.

Usage

When RA suppress function is enabled, no RA/RS packet should be sent from this interface even a RS packet is received.

Examples

This example shows how to enable the RA suppress function:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 nd ra suppress

This example shows how to disable the RA suppress function:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ipv6 nd ra suppress

Related Commands

ipv6 nd ra interval
ipv6 nd ra lifetime

5.2.8 ipv6 nd ra mtu suppress

Command Purpose

Use this command to enable the RA MTU suppress function. To disable this function, use the no form of this command.

Command Syntax

ipv6 nd ra mtu suppress
no ipv6 nd ra mtu suppress

Command Mode

Interface Configuration

Default

By default, RA MTU suppress is disabled.

Usage

When RA MTU suppress function is enabled, no MTU option should be sent in the RA packets from this interface.
Examples

This example shows how to enable the RA MTU suppress function:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 nd ra mtu suppress

This example shows how to disable the RA MTU suppress function:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ipv6 nd ra mtu suppress

Related Commands

None

5.2.9 ipv6 nd ra interval

Command Purpose

Use this command to set the interval of the RA packets. To restore the default configuration, use the no form of this command.

Command Syntax

ipv6 nd ra interval MAX (MIN)
no ipv6 nd ra interval

Command Mode

Interface Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAX</td>
<td>RA max interval (sec).</td>
<td>4-1800 seconds</td>
</tr>
<tr>
<td>MIN</td>
<td>RA min interval (sec).</td>
<td>3-1350 seconds</td>
</tr>
</tbody>
</table>

Default

By default, MAX interval should be 600 second; MIN interval should be 0.33*MAX.

Usage

The valid range should be between 4 and 1800 second for the max value. The valid range should be between 3 and 0.75 * MAX for the minimum value. If the minimum value is not specified, it should be 0.33*MAX when MAX >= 9, and it should be equal to the MAX when MAX < 9.

Examples

This example shows how to set the RA interval:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 nd ra interval 300

Related Commands

ipv6 nd ra suppress
ipv6 nd ra lifetime

5.2.10 ipv6 nd ra lifetime

Command Purpose

Use this command to set the life time of the RA packets. To restore the default configuration, use the no form of this command.
**Command Syntax**

.ipv6 nd ra lifetime \(LIFE\_TIME\)
.no ipv6 nd ra lifetime

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>(LIFE_TIME)</td>
<td>Set IPv6 router advertisement lifetime.</td>
<td>0-9000 seconds</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

By default, RA life time is 3* MAX RA interval.

**Usage**

None

**Examples**

This example shows how to set the ra life time:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 nd ra lifetime 1000
```

**Related Commands**

.ipv6 nd ra suppress
.ipv6 nd ra interval

---

### 5.2.11 ipv6 nd reachable-time

**Command Purpose**

Use this command to set reachable time of the neighbor entries.

To restore the default configuration, use the no form of this command

**Command Syntax**

.ipv6 nd reachable-time \(REACHABLE\_TIME\)
.no ipv6 nd reachable-time

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>(REACHABLE_TIME)</td>
<td>Reachability time in milliseconds.</td>
<td>0-3600000 milliseconds</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

By default, the value is 30000 ms

**Usage**

A reachable time 0 means to restore the default value 30000.

After the reachable time expired, the neighbor entries which state is "REACH" should change to "STALE".
Examples

This example shows how to set the reachable time:
```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 nd reachable-time 3600000
```

Related Commands

None

5.2.12  ipv6 nd managed-config-flag

Command Purpose

Use this command to set "Managed address configuration" flag. To unset this configuration, use the no form of this command.

Command Syntax

```
ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag
```

Command Mode

Interface Configuration

Default

By default, the "Managed address configuration" is not set.

Usage

None

Examples

This example shows how to set the "Managed address configuration" flag:
```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 nd managed-config-flag
```

Related Commands

ipv6 nd other-config-flag

5.2.13  ipv6 nd other-config-flag

Command Purpose

Use this command to set the “Other configuration” flag. To unset this configuration, use the no form of this command.

Command Syntax

```
ipv6 nd other-config-flag
no ipv6 nd other-config-flag
```

Command Mode

Interface Configuration

Default

By default, the "Other configuration" flag is not set.
### 5.2.14 ipv6 nd prefix

**Command Purpose**

Use this command to set prefix for route advertise (RA).

To unset a prefix to advertise, use the no form of this command.

**Command Syntax**

```
ipv6 nd prefix IPv6_PREFIX ( VALID_TIME | infinite ) ( PERFERRED_TIME | infinite ) ( | off-link | no-autoconfig )
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6_PREFIX</td>
<td>Configure IPv6 routing prefix advertisement. IPv6 prefix in X:X::X:X/M format</td>
<td>IPv6 Address and mask length</td>
</tr>
<tr>
<td>VALID_TIME</td>
<td>Valid lifetime.</td>
<td>0-4294967295 second</td>
</tr>
<tr>
<td>PERFERRED_TIME</td>
<td>Preferred lifetime.</td>
<td>0-4294967295 second</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

The valid range of valid life time should be between 0 and 4294967295 seconds. User can also use the keyword "infinite" to indicate the value 4294967295(0xFFFFFFFF). The default value should be 2592000 seconds (30 days).

The valid range of preferred life time should be between 0 and 4294967295 seconds. User can also use the keyword "infinite" to indicate the value 4294967295(0xFFFFFFFF). The default value should be 604800 seconds (7 days).

**Usage**

None

**Examples**

This example shows how to set the prefix:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 nd prefix 2001::1/64
```

**Related Commands**

- show ipv6 interface IFNAME prefix
- ipv6 nd managed-config-flag
5.2.15  show ipv6 interface IFNAME prefix

Command Purpose

Use this command to show the prefix for route advertise (RA) on the specified interface.

Command Syntax

show ipv6 interface IFNAME prefix

Command Mode

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Name of the interface to show</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

Privileged EXEC

Default

None

Usage

None

Examples

This example shows the result of this command:
Switch# show ipv6 interface eth-0-1 prefix

Related Commands

ipv6 nd prefix

5.2.16  show ipv6 neighbors

Command Purpose

Use this command to show all ipv6 neighbor entries.

Command Syntax

show ipv6 neighbors ( dynamic | static | interface IFNAME | IPV6_ADDR | statistics | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface IFNAME</td>
<td>Name of the interface to show</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
<tr>
<td>IPV6_ADDR</td>
<td>IPv6 address in X::X::X::X format</td>
<td>IPv6 Address</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

Neighbor entries should be able to show globally, by interface, or by prefix. Dynamic and static entries can be displayed separately.
Examples

This example shows the result of this command:
Switch# show ipv6 neighbors

<table>
<thead>
<tr>
<th>IPv6 address</th>
<th>Age</th>
<th>Link-Layer Addr</th>
<th>State</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001::2</td>
<td>7</td>
<td>40f2.fd60.ac00</td>
<td>REACH</td>
<td>eth-0-9</td>
</tr>
<tr>
<td>fe80::42f2:fdff:fe60:ac00</td>
<td>6</td>
<td>40f2.fd60.ac00</td>
<td>STALE</td>
<td>eth-0-9</td>
</tr>
</tbody>
</table>

Related Commands

ipv6 neighbor

5.2.17 debug ipv6 nd

Command Purpose

Use this command to open the debug of ipv6 ND feature. To close the debug of ipv6 ND feature, use the no form of this command.

Command Syntax

devup ipv6 nd ( packet | events | error | dump | info | all )
no debug ipv6 nd ( packet | events | error | dump | info | all )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>packet</td>
<td>IPv6 ND packet</td>
<td>-</td>
</tr>
<tr>
<td>events</td>
<td>IPv6 ND events</td>
<td>-</td>
</tr>
<tr>
<td>error</td>
<td>IPv6 ND Error message</td>
<td>-</td>
</tr>
<tr>
<td>dump</td>
<td>Dump message in hex format</td>
<td>-</td>
</tr>
<tr>
<td>info</td>
<td>IPv6 ND information</td>
<td>-</td>
</tr>
<tr>
<td>all</td>
<td>Turn all debugging on</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

By default, the ipv6 nd debug is closed.

Usage

None

Examples

This example shows how to open the ipv6 ND debug:
Switch# debug ipv6 nd all
Switch# terminal monitor

Related Commands

None
5.3 DHCPv6 Relay Commands

5.3.1 dhcpv6 relay

Command Purpose
To enable the DHCPv6 relay service, use the dhcpv6 relay command in global configuration mode.
To disable this function, use the no form of this command.

Command Syntax
```
dhcpv6 relay
no dhcpv6 relay
```

Command Mode
Global Configuration

Default
DHCPv6 relay is disabled.

Usage
The DHCPv6 service must be enabled with the dhcpv6 service command before DHCPv6 relay service can be used.

Examples
The following example shows how to enable DHCPv6 relay agent:
```
Switch# configure terminal
Switch(config)# dhcpv6 relay
```

Related Commands
service dhcpv6

5.3.2 dhcpv6-server (global)

Command Purpose
To create a DHCPv6 server group, use the dhcpv6-server command in global configuration mode.
To remove a DHCPv6 server group, use the no form of this command.

Command Syntax
```
dhcpv6-server NUMBER IPV6_ADDR interface IFNAME
no dhcpv6-server NUMBER ( IPV6_ADDR ( interface IFNAME | ) | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>Number of the DHCPv6 server group. The range is from 1 to 16</td>
<td>1-16</td>
</tr>
<tr>
<td>IPV6_ADDR</td>
<td>The IPv6 address list of the DHCPv6 server. The range in number of the servers in a list is 1 to 8</td>
<td>IPv6 address</td>
</tr>
<tr>
<td>IFNAME</td>
<td>The name of supported interface</td>
<td>Support physical/aggregation/vlan ports</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
No DHCPv6 server group is defined.
Usage

This command is used to specify the remote DHCPv6 server.

Examples

The following example shows how to configure dhcpv6-server group globally:

```
Switch# configure terminal
Switch(config)# dhcpv6-server 1 2001:1::1
Switch(config)# dhcpv6-server 1 fe80::1 interface vlan1
```

Related Commands

service dhcpv6
dhcpv6-server (interface)

5.3.3 dhcpv6-server (interface)

Command Purpose

To add an interface into a DHCPv6 server group, use the dhcpv6-server command in interface configuration mode. To remove this interface from the DHCPv6 server group, use the no form of this command.

Command Syntax

```
dhcpv6-server NUMBER
no dhcpv6-server
```

Command Mode

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>Number of the DHCPv6 server group.</td>
<td>1-16</td>
</tr>
</tbody>
</table>

Interface Configuration

Default

No DHCPv6 server group is configured for the interface.

Usage

This command is used to specify DHCPv6 server group which is configured by the command dhcpv6-server in global mode.

Examples

The following example shows how to configure dhcpv6-server group for interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dhcpv6-server 1
```

Related Commands

service dhcpv6

5.3.4 dhcpv6 relay remote-id option

Command Purpose

To enable remote-id option, use the dhcpv6 relay remote-id option command in global configuration mode. To disable remote-id option, use the no form of this command.

Command Syntax

```
dhcpv6 relay remote-id option
no dhcpv6 relay remote-id option
```
Command Mode
Global Configuration

Default
Remote-id option is not added into DHCPv6 RELAY_FORW packet sent by relay.

Usage
None

Examples
The following example shows how to enable remote-id option:
Switch# configure terminal
Switch(config)# dhcpv6 relay remote-id option

Related Commands
dhcpv6 relay remote-id format

5.3.5 dhcpv6 relay remote-id format

Command Purpose
To specify the format of remote-id, use the dhcpv6 relay remote-id format command in global configuration mode. To restore the default format, use the no form of this command.

Command Syntax
dhcpv6 relay remote-id format { vlan | ifname | duid }
no dhcpv6 relay remote-id format

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>The ID of the vlan attached by client</td>
<td></td>
</tr>
<tr>
<td>ifname</td>
<td>The name of the interface received packet from client</td>
<td></td>
</tr>
<tr>
<td>duid</td>
<td>The duid of relay</td>
<td></td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
The remote-id format is "duid:ifname:"

Usage
The format of remote-id can be a combination of vlan, interface name, DUID. This command specifies the existing keywords in the combination.

Examples
The following example shows how to specify the format of remote-id:
Switch# configure terminal
Switch(config)# dhcpv6 relay remote-id format vlan

Related Commands
dhcpv6 relay remote-id option
5.3.6 dhcpv6 relay pd route

Command Purpose
To enable learning route from prefix-delegation option, use the dhcpv6 relay pd route command in global configuration. To disable the function, use the no form of this command.

Command Syntax

dhcpv6 relay pd route
no dhcpv6 relay pd route

Command Mode
Global Configuration

Default
The DHCPv6 relay won't learn prefix-delegation route.

Usage
The DHCPv6 relay can learn route from prefix delegated by server to client. This kind of route should not replace static one. Use this command to enable this function.

Examples
The following example shows how to enable learning route from prefix-delegation option:
Switch# configure terminal
Switch(config)# dhcpv6 relay pd route

Related Commands

clear dhcpv6 relay pd route
dhcpv6 relay pd route distance

5.3.7 dhcpv6 relay pd route distance

Command Purpose
To configure the default distance for route learned by relay, use the dhcpv6 relay pd route distance command in global configuration. To restore the default value, use the no form of this command.

Command Syntax

dhcpv6 relay pd route distance DISTANCE
no dhcpv6 relay pd route distance

Command Mode

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISTANCE</td>
<td>The default distance for route learned by relay</td>
<td>1-255</td>
</tr>
</tbody>
</table>

Global Configuration

Default
The default value of distance is 254.

Usage
Use this command to configure the distance of the route learned by relay from prefix-delegation.
Examples

The following example shows how to configure the distance of route added by DHCPv6 relay:

```
Switch# configure terminal
Switch(config)# dhcpv6 relay pd route distance 233
```

Related Commands
dhcpv6 relay pd route

5.3.8 service dhcpv6

Command Purpose

To enable the Dynamic Host Configuration Protocol (DHCPV6) relay agent features on your router, use the service dhcpv6 command in global configuration mode.

To disable the DHCPV6 relay agent features, use the no form of this command.

Command Syntax

```
service dhcpv6 enable
service dhcpv6 disable
```

Command Mode

Global Configuration

Default

DHCPV6 service is disabled globally.

Usage

Only the main DHCPV6 service is enabled by the service dhcpv6 command, other DHCPV6 services could be used, such as dhcpv6 relay.

Examples

The following example shows how to enable DHCPV6 service globally:

```
Switch# configure terminal
Switch(config)# service dhcpv6 enable
```

Related Commands
dhcpv6 relay

5.3.9 debug dhcpv6 relay

Command Purpose

Use this command to turn on the debug switches of DHCPV6 relay module.

To restore the default, use the no form of this command

Command Syntax

```
debug dhcpv6 relay { events | error | dump | packet | all }
no debug dhcpv6 relay { events | error | dump | packet | all }
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>events</td>
<td>Relay events</td>
<td>-</td>
</tr>
<tr>
<td>error</td>
<td>Error DHCP message</td>
<td>-</td>
</tr>
<tr>
<td>packet</td>
<td>DHCP message fields</td>
<td>-</td>
</tr>
<tr>
<td>dump</td>
<td>Dump message in hex format</td>
<td>-</td>
</tr>
<tr>
<td>all</td>
<td>Turn all debugging on</td>
<td>-</td>
</tr>
</tbody>
</table>
**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
Use command "terminal monitor" to make debug messages print on the VTY immediately.
Use command "show logging buffer" to check the debug messages in the logging buffer.

**Examples**
The following is sample to open dhcpv6 relay debug switches:
```
Switch# debug dhcpv6 relay all
```

**Related Commands**
terminal monitor
show logging buffer

5.3.10 show dhcpv6-server

**Command Purpose**
To display the DHCPv6 server groups, use the show dhcpv6-server command in privileged EXEC mode.

**Command Syntax**
```
show dhcpv6-server
```

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
This command is used to display all the DHCPv6 server groups configured with command dhcpv6-server in global mode.

**Examples**
The following example shows how to display dhcpv6-server group information:
```
Switch# show dhcpv6-server

DHCPv6 server group information:  
================================================================================  
group 1 ipv6 address list:  
[1] 2001:1::1  
```

**Related Commands**
dhcpv6-server (global)

5.3.11 show dhcpv6 relay interfaces

**Command Purpose**
To display to which dhcpv6-server group the interface belongs, use the show dhcpv6 relay interfaces command in privileged EXEC mode.

**Command Syntax**
```
show dhcpv6 relay interfaces
```

```
```
Command Mode
Privileged EXEC

Default
None

Usage
This command is used to display the interface which is confined DHCPv6 relay.

Examples
The following example shows how to display dhcpv6 relay interfaces information:

```
Switch# show dhcpv6 relay interfaces
List of DHCPv6 relay enabled interface(s):
  DHCPv6 relay service status: enabled
  Interface Name        DHCPv6 server group
  eth-0-1               1
```

Related Commands
show dhcpv6-server

5.3.12 show dhcpv6 relay pd client

Command Purpose
To display the result of DHCPv6 relay's prefix-delegation route function, use the show dhcpv6 relay pd client command in privileged EXEC mode.

Command Syntax
```
show dhcpv6 relay pd client
```

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following example shows how to display information of prefix-delegation route:

```
Switch# show dhcpv6 relay pd client
DHCPv6 prefix-delegation client information:
=================================================================================
Interface        : vlan2
Client DUID       : 0001000117e9357b606da18230
Client IPv6 address: fe80:626d:a1ff:fe82:300
  IA ID           : a18230
  IA Prefix       : 2002:2:10::/64
  preferred/max lifetime : 280/300
  expired time     : 2012-09-17 11:43:59
```
Related Commands

dhcpv6 relay pd route
dhcpv6 relay pd route distance

5.3.13  show dhcpv6 relay statistics

Command Purpose
To display the statistics of DHCPv6 packets relayed by the switch, use the show dhcpv6 relay statistics command in privileged EXEC mode.

Command Syntax
show dhcpv6 relay statistics

Command Mode
Privileged EXEC

Default
None

Usage
This command is used to display detail DHCPv6 statistics which processed by the switch.

Examples
The following example shows how to display DHCPv6 relay statistics:

Switch# show dhcpv6 relay statistics

DHCPv6 relay packet statistics:

<table>
<thead>
<tr>
<th></th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client relayed packets</td>
<td>48</td>
</tr>
<tr>
<td>Server relayed packets</td>
<td>48</td>
</tr>
<tr>
<td>Client error packets</td>
<td>0</td>
</tr>
<tr>
<td>Server error packets</td>
<td>0</td>
</tr>
</tbody>
</table>

Related Commands

clear dhcpv6 relay statistics

5.3.14  clear dhcpv6 relay statistics

Command Purpose
To reset the statistics of DHCPv6 packets relayed by the switch, use the clear dhcpv6 relay statistics command in privileged EXEC mode.

Command Syntax
clear dhcpv6 relay statistics

Command Mode
Privileged EXEC

Default
None

Usage
This command is used to reset DHCPv6 statistics.
Examples
The following example shows how to clear DHCPv6 relay statistics:
Switch# clear dhcpv6 relay statistics

Related Commands
show dhcpv6 relay statistics

5.3.15 clear dhcpv6 relay pd route

Command Purpose
To clear the route learned by DHCPv6 relay from prefix-delegation, use the clear dhcpv6 relay pd route command in privileged EXEC mode.

Command Syntax

```
clear dhcpv6 relay pd route (prefix | prefix-list) (interface | IFNAME) (IPv6_ADDR)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PREFIX</td>
<td>The prefix delegated to client</td>
<td>IPv6 Address and mask length in XX::XX/M format</td>
</tr>
<tr>
<td>IPV6_ADDR</td>
<td>The IPv6 address of PD client</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>IFNAME</td>
<td>The name of supported interface</td>
<td>Support physical/aggregation/vlan ports</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
If no parameter is specified, all route will be cleared.

Examples
The following example shows how to clear route learned by DHCPv6 relay:
Switch# clear dhcpv6 relay pd route interface eth-0-1

Related Commands
dhcpv6 relay pd route
show dhcpv6 relay pd client
Chapter 6 IP Routing Commands

6.1 IP Unicast-Routing Commands

6.1.1 ip address

Command Purpose

To set a primary or secondary IP address for an interface, use the ip address command in interface configuration mode. To remove an IP address or disable IP processing, use the no form of this command.

Command Syntax

```
ip address (ADDRESS WILDCARD-MASK | ADDRESS/PREFIX-LENGTH) { secondary }
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADDRESS</td>
<td>IPv4 address of the interface</td>
<td>IPv4 address</td>
</tr>
<tr>
<td>WILDCARD-MASK</td>
<td>Mask for the associated IP subnet</td>
<td>Mask in IPv4 address format</td>
</tr>
<tr>
<td>PREFIX-LENGTH</td>
<td>Prefix length of the address</td>
<td>1-32</td>
</tr>
<tr>
<td>secondary</td>
<td>(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

No IP address is defined for the interface.

Usage

An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the switch always use the primary IP address. Therefore, all switches and access servers on a segment should share the same primary network number.

Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) mask request message. Switch respond to this request with an ICMP mask reply message.

You can disable IP processing on a particular interface by removing its IP address with the no ip address command. If the software detects another host using one of its IP addresses, it will print an error message on the console.

The optional secondary keyword allows you to specify up to 8 secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.

Secondary IP addresses can be used in a variety of situations. The following are the most common applications:
There may not be enough host addresses for a particular network segment. For example, your subnet allows up to 254 hosts per logical subnet, but on one physical subnet you need 300 host addresses. Using secondary IP addresses on the switches or access servers allows you to have two logical subnets using one physical subnet.

Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnet and router-based network. Switches on an older, bridged segment can be easily made aware that many subnets are on that segment.

Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is extended, or layered on top of the second network using secondary addresses.

**Examples**

In the following example, 10.108.1.27 is the primary address and 192.31.7.17 and 192.31.8.17 are secondary addresses for eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ip address 10.108.1.27 255.255.255.0
Switch(config-if)# ip address 192.31.7.17/24 secondary
Switch(config-if)# ip address 192.31.8.17 255.255.255.0 secondary
```

**Related Commands**

None

### 6.1.2 `ip icmp error-interval`

**Command Purpose**

To set the interval of ICMP error messages generated by the switch, use the `ip icmp error-interval` command in global configuration mode. To restore the default value, use the no form of this command.

**Command Syntax**

```
ip icmp error-interval INTERVAL
no ip icmp error-interval
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>The interval in milliseconds.</td>
<td>0 - 2147483647 milliseconds</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

Default is 1000 milliseconds.
Usage
None

Example
In the following example, user sets the error interval to 10 seconds, which means only one ICMP error message was generated per 10 seconds:

```
Switch# configure terminal
Switch(config)# ip icmp error-interval 10000
```

Related Commands
ip redirects
ip unreachable

6.1.3 ip redirects

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

Command Syntax
```
ip redirects
no ip redirects
```

Command Mode
Interface Configuration

Default
IP redirect is enabled by default.

Usage
None

Examples
In the following example, users disable to send the ICMP redirect message:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1/24
Switch(config-if)# no ip redirects
```

Related Commands
ip unreachable
ip icmp error-interval
6.1.4 ip 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

6.1.5 ip verify unicast reverse-path

Command Purpose

To enable RPF check to the interface, use the command ip verify unicast reverse-path in interface configuration mode. To restore the default value, use the no form of this command.
**Command Syntax**

ip verify unicast reverse-path  
no ip verify unicast reverse-path

**Command Mode**

Interface Configuration

**Default**

RPF check is disabled by default.

**Usage**

None

**Examples**

In the following example, users enable RPF check in interface eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1/24
Switch(config-if)# ip verify unicast reverse-path
```

**Related Commands**

- ip redirects
- ip icmp error-interval

**6.1.6 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
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-ADDRESS</td>
<td>Router ID in IP address format</td>
<td>IPv4 address</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

No router ID is defined.

**Usage**

You can configure an arbitrary value in the IP address format for each switch. However, each router ID must be unique.

**Examples**

The following example specifies a fixed router-id:

```
Switch# configure terminal
Switch(config)# router-id 1.1.1.1
```

**Related Commands**

router-id (router)

### 6.1.7 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 | PREFIX/PREFIX-LENGTH) (NH-ADDRESS | IFNAME) (DISTANCE | ) (track NUMBER | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF NAME</td>
<td>VRF instance name</td>
<td>A string up to 16 characters</td>
</tr>
<tr>
<td>PREFIX</td>
<td>IP route prefix for the destination</td>
<td>IPv4 address</td>
</tr>
<tr>
<td>MASK</td>
<td>Prefix mask for the destination</td>
<td>Mask in IPv4 address format</td>
</tr>
<tr>
<td>PREFIX-LENGTH</td>
<td>Prefix length for the destination</td>
<td>1-32</td>
</tr>
<tr>
<td>NH-ADDRESS</td>
<td>IP address of the next hop that can be used to reach that network</td>
<td>IPv4 address</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Interface name of the next hop that can be used to reach that network.</td>
<td>Only support tunnel and null interface</td>
</tr>
<tr>
<td>DISTANCE</td>
<td>(Optional) An administrative distance. The default administrative distance for a static route is 1</td>
<td>1-255</td>
</tr>
<tr>
<td>track NUMBER</td>
<td>Specify the ID of track object</td>
<td>1-500</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration
Default
No static routes are established.

Usage
The establishment of a static route is appropriate when the switch cannot dynamically build a route to the destination.

Examples
The following example establishes a static route:

```
Switch# configure terminal
Switch(config)# ip route 172.31.0.0 255.255.0.0 172.31.6.6
```

The following example establishes a static route which nexthop is blackhole:

```
Switch# configure terminal
Switch(config)# ip route 10.1.1.1/32 null 0
```

Related Commands
show ip route

6.1.8 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 |)  
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF NAME</td>
<td>VRF instance name</td>
<td>A string up to 15 characters</td>
</tr>
<tr>
<td>IP-ADDRESS</td>
<td>(Optional) Address about which routing information should be displayed</td>
<td>IPv4 address</td>
</tr>
<tr>
<td>PREFIX</td>
<td>IP route prefix</td>
<td>IPv4 address</td>
</tr>
<tr>
<td>PREFIX-LENGTH</td>
<td>Prefix length for the route</td>
<td>1-32</td>
</tr>
<tr>
<td>PROTOCOL</td>
<td>(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.</td>
<td>bgp/connected/isis/ospf/rip/static</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None
Usage

You can display all active dynamic and static routes with both the show ip route and show ip route static commands after these active routes are added in the main routing table.

Examples

The following is sample output from the show ip route command when entered without an address:

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       [ ] - [AD/Metric]
       * - candidate default

O    1.1.1.0/24 [110/2] via 10.10.1.1, eth-0-23, 00:34:17
O    2.2.2.0/24 [110/3] via 10.10.1.1, eth-0-23, 00:17:26
C    10.10.1.0/24 is directly connected, eth-0-23
C    10.10.1.23/32 is in local loopback, eth-0-23
O    10.10.2.0/24 [110/2] via 10.10.1.1, eth-0-23, 00:17:26
O    10.10.3.0/24 [110/3] via 10.10.1.1, eth-0-23, 00:17:26
```

Related Commands

ip route
show ip route database

6.1.9 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 |)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF NAME</td>
<td>VRF instance name</td>
<td>A string up to 15 characters</td>
</tr>
<tr>
<td>PROTOCOL</td>
<td>(Optional) The name of a routing protocol, or the</td>
<td>bgp/connected/isis/ospf/rip/static</td>
</tr>
<tr>
<td></td>
<td>keyword connected, static, or summary. If you specify a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>routing protocol, use one of the following keywords: bgp,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospf, or rip.</td>
<td></td>
</tr>
</tbody>
</table>
Command Mode

Privileged EXEC

Default

None

Usage

You can display all active dynamic and static routes with both the show ip route database and show ip route database static commands after these active routes are added in the Routing Information Base (RIB).

Examples

The following is sample output from the show ip route database command:

```
Switch# show ip route database

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
           O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
           E1 - OSPF external type 1, E2 - OSPF external type 2
     [?] - [AD/Metric]
        > - selected route, * - FIB route, p - stale info

O  *> 1.1.1.0/24 [110/2] via 10.10.1.1, eth-0-23, 00:48:58
O  *> 2.2.2.0/24 [110/3] via 10.10.1.1, eth-0-23, 00:32:07
S  6.6.6.0/24 [1/0] via 3.3.3.3 inactive
C  *> 10.10.1.0/24 is directly connected, eth-0-23
C  *> 10.10.1.23/32 is in local loopback, eth-0-23
O  *> 10.10.2.0/24 [110/2] via 10.10.1.1, eth-0-23, 00:32:07
O  *> 10.10.3.0/24 [110/3] via 10.10.1.1, eth-0-23, 00:32:07
```

Related Commands

ip route
show ip route

6.1.10  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 |)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF NAME</td>
<td>VRF instance name</td>
<td>A string up to 15 characters</td>
</tr>
<tr>
<td>PROTOCOL</td>
<td>(Optional) The name of a routing protocol. If you specify a routing protocol, use one of the following keywords: bgp, ospf, isis and rip.</td>
<td>bgp/ospf/rip/isis</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

The information displayed by the show ip protocols command is useful in debugging routing operations. Information in the Routing Information Sources field of the show ip protocols output can help you identify a switch suspected of delivering bad routing information.

Examples

The following is sample output from the show ip protocols command:

```
Switch# show ip protocols
Routing Protocol is “ospf 0”
   Redistributing:
   Routing for Networks:
      3.3.3.0/24
      10.10.1.0/24
      10.10.4.0/24
   Distance: (default is 110)
```

Related Commands

show ip route
6.1.11 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF NAME</td>
<td>VRF instance name</td>
<td>A string up to 15 characters</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show ip route summary command:

Switch# show ip route summary

IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 8
Route source networks connected 2 static 1 Total 3

Related Commands

show ip route
6.1.12 show ip route add-fib-fail

Command Purpose

Use this command to display the routes which cannot 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 | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>number of add-fib-fail route entries</td>
<td>-</td>
</tr>
</tbody>
</table>

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 hardware resource limit, this route is not able to forward any packets. You could delete and reconfigure this routing when some hardware resource is free.

Examples

The following is sample output from the show ip route add-fib-fail command:

```
Switch# show ip route add-fib-fail
======================================
VRF  Route
default  1.1.1.1/32
default  1.1.1.0/24
test  2.2.2.2/32
test  2.2.2.0/24
```

Related Commands

show ip route
6.1.13 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>COUNT</td>
<td>maximum static routes in system</td>
<td>The range is &lt;1-65535&gt;, default value is 1024</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

1024

Usage

Users should not configure the maximum static routes more than system profile of FIB. Also, users should not configure the maximum static routes less than the current static routes count.

Examples

The following example displays how to change maximum static routes to 10:

Switch# confi terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# max-static-routes 10

Related Commands

show ip route summary

6.1.14 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

**6.1.15  ecmp load-balance-mode dynamic**

**Command Purpose**

Use this command to configure ecmp dynamic load balance.
Command Syntax

ecmp load-balance-mode dynamic
no ecmp load-balance-mode dynamic

Command Mode

Global Configuration

Default

Static load balance mode

Usage

When configure or cancel ecmp load balance, the route information must be empty.

Examples

The following example displays how to configure ecmp dynamic load balance:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ecmp load-balance-mode dynamic

Related Commands

None

6.1.16 ecmp load-balance-mode dynamic (efd-only|tcp-only)

Command Purpose

Use this command to configure only tcp flows do ecmp dynamic load or only efd flows do ecmp dynamic load.

Command Syntax

ecmp load-balance-mode dynamic (efd-only | tcp-only )
no ecmp load-balance-mode dynamic

Command Mode

Global Configuration
Default

Flows of every type can do ecmp dynamic load.

Usage

None

Examples

The following example displays how to configure only tcp flows do ecmp dynamic load:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ecmp load-balance-mode dynamic tcp-only

Related Commands

None

6.1.17  ecmp load-balance-mode static

Command Purpose

Use this command to configure ecmp static load balance.

Command Syntax

ecmp load-balance-mode static

Command Mode

Global Configuration

Default

None

Usage

When configure ecmp load balance, the route information must be empty.
Examples

The following example displays how to configure ecmp static load balance:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ecmp load-balance-mode static
```

Related Commands

None

6.1.18 ecmp load-balance-mode static self-healing

Command Purpose

Use this command to configure ecmp self-healing load balance.

Command Syntax

```
ecmp load-balance-mode static self-healing
no ecmp load-balance-mode static self-healing
```

Command Mode

Global Configuration

Default

None

Usage

None

Examples

The following example displays how to configure ecmp self-healing load balance:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ecmp load-balance-mode static self-healing
```

Related Commands

None

6.1.19 ecmp load-balance-mode round-robin

Command Purpose

Use this command to configure ecmp round robin load balance.
Command Syntax

ecmp load-balance-mode round-robin A.B.C.D/M
no ecmp load-balance-mode round-robin A.B.C.D/M

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D/M</td>
<td>IP destination prefix (e.g. 10.0.0.0/8), vrf private route isn’t support RR</td>
<td>IPv4 address and mask length in A.B.C.D/M format</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

When configure or cancel ecmp load balance, the route information must be empty.

Examples

The following example displays how to configure ecmp round robin load balance:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ecmp load-balance-mode round-robin 1.1.1.0/24

Related Commands

None

6.1.20 ecmp hash-field-select

Command Purpose

Use this command to configure to use which fields to compute ecmp hash.

Command Syntax

ecmp hash-field-select { ipda | ipsa | ip-protocol | sourceport | destport | vxlan-vni | nvgre-vsid | inner-ipda | inner-ipsa | inner-ip-protocol | inner-sourceport | inner-destport }
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipda</td>
<td>Destination IP address</td>
<td>-</td>
</tr>
<tr>
<td>ipsa</td>
<td>Source IP address</td>
<td>-</td>
</tr>
<tr>
<td>ip-protocol</td>
<td>Ip-protocol</td>
<td>-</td>
</tr>
<tr>
<td>sourceport</td>
<td>Source port</td>
<td>-</td>
</tr>
<tr>
<td>destport</td>
<td>Destination port</td>
<td>-</td>
</tr>
<tr>
<td>vxlan-vni</td>
<td>Vni of vxlan</td>
<td>-</td>
</tr>
<tr>
<td>nvgre-vsid</td>
<td>Vsid of nvgre</td>
<td>-</td>
</tr>
<tr>
<td>inner-ipda</td>
<td>Inner destination IP address</td>
<td>-</td>
</tr>
<tr>
<td>inner-ipsa</td>
<td>Inner source IP address</td>
<td>-</td>
</tr>
<tr>
<td>inner-ip-protocol</td>
<td>Inner ip-protocol</td>
<td>-</td>
</tr>
<tr>
<td>inner-sourceport</td>
<td>Inner source port</td>
<td>-</td>
</tr>
<tr>
<td>inner-destport</td>
<td>Inner destination port</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

ipsa ipda(outer header)

**Usage**

None

**Examples**

The following example shows how to use ipsa,ipda and inner-ipda to compute ecmp hash:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ecmp hash-field-select ipsa ipda inner-ipda
Switch(config)#
```

**Related Commands**

None

6.1.21 show ecmp information

**Command Purpose**

Use this command to display ecmp configure information.
Command Syntax

show ecmp information

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows the output of the command:

Switch# show ecmp information

ECMP load balance enable mode: Static
ECMP hash-field-select:
  ipsa ipda
  inner-ipda

Related Commands

None

6.1.22  ecmp load-balance hash-arithmetic

Command Purpose

Use this command to configure ecmp hash arithmetic.
Use the no format of this command to restored the default value.

Command Syntax

ecmp load-balance hash-arithmetic ( xor | crc )
nocmp load-balance hash-arithmetic

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>xor</td>
<td>XOR hash algorithm</td>
<td>-</td>
</tr>
<tr>
<td>crc</td>
<td>CRC hash algorithm</td>
<td>-</td>
</tr>
</tbody>
</table>
Command Mode

Global Configuration

Default

XOR

Usage

None

Examples

The following example displays how to configure ecmp load balance hash arithmetic:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ecmp load-balance
Switch(config)# ecmp load-balance hash-arithmetic crc

Related Commands

None

6.2 RIP Commands

6.2.1 default-information originate (RIP)

Command Purpose

To generate a default route into Routing Information Protocol (RIP), use the default-information originate command in router configuration mode. To disable this feature, use the no form of this command.

Command Syntax

default-information originate ( route-map | )

no default-information originate

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-map</td>
<td>Route map reference</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration
Default

None

Usage

The route originated will only be learned by RIP neighbor, and this route is not configured in FIB.

Examples

The following example originates a default route:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# version 2
Switch(config-router)# network 192.168.16.0/24
Switch(config-router)# default-information originate
```

Related Commands

None

6.2.2 default-metric (RIP)

Command Purpose

To set default metric values for Routing Information Protocol (RIP), use the default-metric command in router configuration mode. To return to the default state, use the no form of this command.

Command Syntax

```
default-metric NUMBER-VALUE
default-metric
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER-VALUE</td>
<td>Default metric value</td>
<td>1-16</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

By default, the metric is set to 1.
Usage

The `default-metric` command is used in conjunction with the `redistribute` router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

Examples

The following example shows a switch using both the RIP and the Open Shortest Path First (OSPF) routing protocols. The example advertises OSPF-derived routes using RIP and assigns the OSPF-derived routes a RIP metric of 10:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# default-metric 10
Switch(config-router)# redistribute ospf
```

Related Commands

`redistribute` (RIP)

6.2.3 distance (RIP)

Command Purpose

To define an administrative distance for routes that are inserted into the routing table, use the `distance` command in router configuration mode. To return the administrative distance to its default distance definition, use the `no` form of this command.

Command Syntax

```
distance DISTANCE PREFIX/PREFIX-LENGTH (ACCESSS-LIST-NAME |)
```

no distance

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISTANCE</td>
<td>Administrative distance</td>
<td>Administrative distance, an integer from 1 to 255 (routes with a distance value of 255 are not installed in the routing table)</td>
</tr>
<tr>
<td>PREFIX</td>
<td>IP prefix for the originator of the incoming routing updates</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PREFIX-LENGTH</td>
<td>Prefix length for the originator</td>
<td>1-32</td>
</tr>
<tr>
<td>ACCESSS-LIST-NAME</td>
<td>(Optional) Named access list to be applied to incoming routing updates</td>
<td>Up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration
**Default**

By default, the distance is 120.

**Usage**

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual switch or a group of switches. Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

When this command is configured, it is applied when a network is being inserted into the routing table. It filters routing updates according to the IP address of the switch that supplies the routing information. It could be used, for example, to filter possibly incorrect routing information from switches that are not under your administrative control. The optional access list name is used to filter router entries in routing update.

**Examples**

The following example set administrative distance 200 for routes that are inserted from 20.20.0.0 network segment:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# network 10.10.0.0/24
Switch(config-router)# network 20.20.0.0/24
Switch(config-router)# distance 200 20.20.0.0/24
```

**Related Commands**

distance (OSPF)

6.2.4 ip rip authentication

**Command Purpose**

To enable authentication for Routing Information Protocol (RIP) Version 2 packets and to specify the set of keys that can be used on an interface, use the ip rip authentication command in interface configuration mode. To prevent authentication, use the no form of this command.

**Command Syntax**

```
ip rip authentication (key-chain NAME-OF-CHAIN | string STRING)
no ip rip authentication (key-chain | string)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>key-chain NAME-OF-CHAIN</td>
<td>Enables authentication and specifies the group of keys that are valid</td>
<td>A String of key chain name</td>
</tr>
<tr>
<td>string STRING</td>
<td>Enables authentication and specifies the authentication string</td>
<td>Up to 16 characters</td>
</tr>
</tbody>
</table>
Command Mode

Interface Configuration

Default

No authentication is provided for RIP packets.

Usage

If neither key chain is configured with the key-chain command nor string is configured with the authentication string command, no authentication is performed on the interface (not even the default authentication). Key chain and authentication string can not be configured on the same interface. If you want configure one, make sure the other is not configured.

Examples

The following example configures the interface to accept and send any key belonging to the key chain named trees:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip rip authentication key-chain trees
```

Related Commands

ip rip authentication mode

6.2.5  ip rip authentication mode

Command Purpose

To specify the type of authentication used in Routing Information Protocol (RIP) Version 2 packets, use the ip rip authentication mode command in interface configuration mode. To restore clear text authentication, use the no form of this command.

Command Syntax

```
ip rip authentication mode ( text | md5 )
no ip rip authentication mode
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>text</td>
<td>Normal text authentication</td>
<td>-</td>
</tr>
<tr>
<td>md5</td>
<td>Keyed Message Digest 5 (MD5)</td>
<td>-</td>
</tr>
</tbody>
</table>
Command Mode

Interface Configuration

Default

Clear text authentication is provided for RIP packets.

Usage

RIP Version 1 does not support authentication.

Examples

The following example configures the interface to use MD5 authentication:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip rip authentication mode md5
```

Related Commands

ip rip authentication key-chain

6.2.6 ip rip receive version

Command Purpose

To specify a Routing Information Protocol (RIP) version to receive on an interface basis, use the `ip rip receive version` command in interface configuration mode. To follow the global version rules, use the no form of this command.

Command Syntax

```
ip rip receive version [1 | 2]
no ip rip receive version
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(Optional) Accepts only RIP Version 1 packets on the interface</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>(Optional) Accepts only RIP Version 2 packets on the interface</td>
<td>-</td>
</tr>
</tbody>
</table>

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 RIPv1 and RIPv2 packets:

```plaintext
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip rip receive version 1 2
```

Related Commands

version (RIP)

6.2.7 `ip rip receive-packet`

Command Purpose

To enable the interface to receive Routing Information Protocol (RIP) packets, use the `ip rip receive-packet` command in interface configuration mode. To disable to receive RIP packets, use the `no` form of this command.

Command Syntax

`ip rip receive-packet`
`no ip rip receive-packet`

Command Mode

Interface Configuration

Default

Receive packet is enabled by default.

Usage

Use this command to enable or disable the capability of receiving RIP packets, whether the network of this interface is added into RIP or not.
Examples

The following example enables the reception of RIP packets:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip rip receive-packet

Related Commands

ip rip receive version

6.2.8 ip rip send version

Command Purpose

To specify a Routing Information Protocol (RIP) version to send on an interface basis, use the ip rip send version command in interface configuration mode. To follow the global version rules, use the no form of this command.

Command Syntax

ip rip send version ( {1 | 2} | 1-compatible )
no ip rip send version

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(Optional) Sends only RIP Version 1 packets out the interface</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>(Optional) Sends only RIP Version 2 packets out the interface</td>
<td>-</td>
</tr>
<tr>
<td>1-compatible</td>
<td>(Optional) Sends RIP Version 2 packets out the interface with broadcast IP address</td>
<td>-</td>
</tr>
</tbody>
</table>

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 configure the interface to send both RIP Version 1 and Version 2 packets:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip rip send version 1 2
```

Related Commands

- `ip rip receive version`

6.2.9 ip rip send-packet

Command Purpose

To enable the interface to send Routing Information Protocol (RIP) packets, use the `ip rip send-packet` command in interface configuration mode. To disable to send RIP packets, use the no form of this command.

Command Syntax

```
ip rip send-packet
no ip rip send-packet
```

Command Mode

- Interface Configuration

Default

Send packet is enabled by default.

Usage

Use this command to enable or disable the capability of sending RIP packets, whether the network of this interface is added into RIP or not.

Examples

The following example enables the transmission of RIP packets:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip rip send-packet
```
Related Commands

ip rip send version

6.2.10 ip rip split-horizon

Command Purpose

To enable the split horizon mechanism for Routing Information Protocol (RIP), use the ip rip split-horizon command in interface configuration mode. To disable the split horizon mechanism, use the no form of this command.

Command Syntax

ip rip split-horizon (poisoned | )
nop ip rip split-horizon

Parameter | Parameter Description | Parameter Value
--- | --- | ---
poisoned | Split horizon with poisoned reverse | -

Command Mode

Interface Configuration

Default

This command is enabled with poisoned reverse by default.

Usage

In general, changing the state of the default for the ip rip split-horizon command is not recommended, unless you are certain that your application requires a change in order to properly advertise routes.

Examples

The following example enables split horizon without poisoned reverse:

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

Related Commands

None
6.2.11  network (RIP)

Command Purpose

To specify a list of networks for the Routing Information Protocol (RIP) routing process, use the network command in router configuration mode. To remove an entry, use the no form of this command.

Command Syntax

network (PREFIX / PREFIX-LENGTH)
no network (PREFIX / PREFIX-LENGTH)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PREFIX</td>
<td>IP route prefix for the network</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PREFIX-LENGTH</td>
<td>Prefix length for the network</td>
<td>1-32</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

No networks are specified.

Usage

There is no limit to the number of network commands you can use on the switch. RIP routing updates will be sent and received only through interfaces on this network.

RIP sends updates to the interfaces in the specified networks. Also, if the network of an interface is not specified, the interface will not be advertised in any RIP update.

Examples

The following example defines RIP as the routing protocol to be used on all interfaces connected to networks 10.99.0.0/16 and 192.168.7.0/24:

Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# network 10.99.0.0/16
Switch(config-router)# network 192.168.7.0/24

Related Commands

router rip
6.2.12 neighbor (RIP)

Command Purpose

To define a neighboring switch with which to exchange routing information, use the neighbor command in router configuration mode. To remove an entry, use the no form of this command.

Command Syntax

```
neighbor IP-ADDRESS
no neighbor IP-ADDRESS
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-ADDRESS</td>
<td>IP address of a peer switch with which routing information will be exchanged</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

No neighboring switches are defined.

Usage

This command permits the point-to-point (non-broadcast) exchange of routing information. When it is used in combination with the passive-interface router configuration command, routing information can be exchanged between a subset of switches and access servers on a LAN.

Multiple neighbor commands can be used to specify additional neighbors or peers.

Examples

In the following example, RIP updates are sent to all interfaces on network 10.108.0.0 except eth-0-1. However, in this case a neighbor switch configuration command is included. This command permits the sending of routing updates to specific neighbors. One copy of the routing update is generated per neighbor:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# network 10.108.0.0/16
Switch(config-router)# passive-interface eth-0-1
Switch(config-router)# neighbor 10.108.20.4
```

Related Commands

```
router rip
```
6.2.13 offset-list (RIP)

Command Purpose

To add an offset to incoming and outgoing metrics to routes learned via Routing Information Protocol (RIP), use the offset-list command in router configuration mode. To remove an offset list, use the no form of this command.

Command Syntax

offset-list ACCESSS-LIST-NAME ( in | out ) METRIC-OFFSET ( IFNAME )
no offset-list ( in | out ) ( IFNAME )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCESSS-LIST-NAME</td>
<td>Named access list to be applied</td>
<td>Up to 40 characters</td>
</tr>
<tr>
<td>in</td>
<td>Applies the access list to incoming metrics</td>
<td>-</td>
</tr>
<tr>
<td>out</td>
<td>Applies the access list to outgoing metrics</td>
<td>-</td>
</tr>
<tr>
<td>METRIC-OFFSET</td>
<td>Positive offset to be applied to metrics for networks matching the access list. If the offset is 0, no action is taken</td>
<td>0-16</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Interface name to which the offset list is applied</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

This command is disabled by default.

Usage

The offset value is added to the routing metric. An offset list with an interface is considered extended and takes precedence over an offset list that is not extended. Therefore, if an entry passes the extended offset list and the normal offset list, the offset of the extended offset list is added to the metric.

Examples

In the following example, the switch applies an offset to the delay component of a switch only to access list 21:

Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# offset-list 21 out 10

Related Commands

None
6.2.14 passive-interface (RIP)

Command Purpose

To disable sending routing updates for the Routing Information Protocol (RIP) on an interface, use the passive-interface command in router configuration mode. To re-enable the sending of routing updates, use the no form of this command.

Command Syntax

```
passive-interface IFNAME
no passive-interface IFNAME
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>The interface name</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

Routing updates are sent on the interface.

Usage

If you disable the sending of routing updates on an interface, the particular subnet will continue to be advertised to other interfaces, and updates from other switches on that interface continue to be received and processed.

Examples

The following example sets the interface eth-0-1 as passive:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# network 10.108.0.0/16
Switch(config-router)# passive-interface eth-0-1
```

Related Commands

router rip

6.2.15 redistribute (RIP)

Command Purpose

To redistribute routes from one routing domain into RIP routing domain, use the redistribute command in router configuration mode. To disable redistribution, use the no form of this command.
Command Syntax

redistribute PROTOCOL { [ metric VALUE ] | route-map WORD }
no redistribute PROTOCOL

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROTOCOL</td>
<td>(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</td>
<td>bgp/ospf/connected/isis/static/isis</td>
</tr>
<tr>
<td>metric VALUE</td>
<td>(Optional) When redistributing other routing process to the RIP process, the default metric is 1 if no metric value is specified</td>
<td>1-16</td>
</tr>
<tr>
<td>route-map</td>
<td>Route map reference</td>
<td>-</td>
</tr>
<tr>
<td>WORD</td>
<td>Pointer to route-map entries</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

Route redistribution is disabled.
Metric metric-value: 1

Usage

The metric value specified in the redistribute command supersedes the metric value specified using the default-metric command.

Examples

The following examples redistribute the static routes into RIP with metric 10:

Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# network 10.108.0.0/16
Switch(config-router)# redistribute static metric 10

Related Commands

default-metric

6.2.16 router rip

Command Purpose

To configure the Routing Information Protocol (RIP) routing process, use the router rip command in global configuration mode. To turn off the RIP routing process, use the no form of this command.
**Command Syntax**

```
router rip
no router rip
```

**Command Mode**

Global Configuration

**Default**

None

**Usage**

None

**Examples**

The following example shows how to enter the RIP routing configuration:

```
Switch# configure terminal
Switch(config)# router rip
```

**Related Commands**

network (RIP)

### 6.2.17 timers basic (RIP)

**Command Purpose**

To adjust Routing Information Protocol (RIP) network timers, use the timers basic command in router configuration mode. To restore the default timers, use the no form of this command.

**Command Syntax**

```
timers basic UPDATE TIMEOUT INVALID
no timers basic
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPDATE</td>
<td>Rate (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol.</td>
<td>&lt;5-2147483647&gt;, default 30s</td>
</tr>
<tr>
<td>TIMEOUT</td>
<td>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.</td>
<td>It is marked inaccessible and advertised as unreachable. &lt;5-2147483647&gt;, default 180s</td>
</tr>
<tr>
<td>INVALID</td>
<td>Time after which an invalid route is removed from RIP routing database.</td>
<td>&lt;5-2147483647&gt;, default 120s</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration
Default

update: 30 seconds
timeout: 180 seconds
invalid: 120 seconds

Usage

The basic timing parameters for RIP are adjustable. Because RIP is executing a distributed, asynchronous routing algorithm, these timers must be the same for all switches and access servers in the network.

In addition, an address family can have explicitly specified timers that apply to that address-family only. The timers basic command must be specified for an address family or the system Default for the timers basic command are used regardless of what is configured for RIP routing.

Examples

The following example sets updates to be broadcast every 5 seconds. If a switch is not heard from in 15 seconds, the route is declared unusable. And after 15 seconds the invalid route will be removed from RIP routing database:

Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# timers basic 5 15 15

Related Commands

None

6.2.18 show ip rip database

Command Purpose

Use this command to display RIP information database.

Command Syntax

show ip rip database (vrf WORD |)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf WORD</td>
<td>VPN Routing/Forwarding instance</td>
<td>Up to 15 characters</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric From</th>
<th>If</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rc 1.1.1.0/24</td>
<td>1</td>
<td>eth-0-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rc 2.2.2.0/24</td>
<td>1</td>
<td>eth-0-2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rc 10.0.0.0/24</td>
<td>1</td>
<td>vlan10</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Related Commands

- show ip rip interface

6.2.19 show ip rip interface

Command Purpose

To display summary information of Routing Information Protocol (RIP) for a specific interface, use the show ip rip interface command in privileged EXEC mode.

Command Syntax

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>The interface name</td>
<td>Support physical/aggregation/loopback/tunnel/vlan interfaces</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None
Usage

None

Examples

The following is sample output from the `show ip rip interface` command:

```
Switch# show ip rip interface eth-0-1
eth-0-1 is up, line protocol is up
   Routing Protocol: RIP
      Receive RIP packets
      Send RIP packets
      Passive interface: Disabled
      Split horizon: Enabled with Poisoned Reversed
   IP interface address:
      1.1.1.1/24
```

Related Commands

- `show ip rip database`

6.2.20  version (RIP)

Command Purpose

To specify a Routing Information Protocol (RIP) version used globally by the router, use the `version` command in router configuration mode. To restore the default value, use the `no` form of this command.

Command Syntax

```
version (1 | 2)
no version
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Specifies RIP Version 1</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>Specifies RIP Version 2</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

System receives RIP Version 1 and Version 2 packets, but sends only Version 2 packets.
Usage

To specify RIP versions used on an interface basis, use the `ip rip receive version` and `ip rip send version` commands.

Examples

The following example enables the software to send and receive RIP Version 2 packets:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# version 2
```

Related Commands

`ip rip receive version`  
`ip rip send version`

6.2.21 distribute-list

Command Purpose

To filter networks in routing updates, use the `distribute-list` command in router configuration mode. To restore the default value, use the `no` form of this command.

Command Syntax

```
distribute-list (prefix | ) WORD ( in | out )
no distribute-list ( prefix | ) WORD ( in | out )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix</td>
<td>Filter prefixes in routing update</td>
<td>-</td>
</tr>
<tr>
<td>WORD</td>
<td>Access-list name</td>
<td>Up to 40 characters</td>
</tr>
<tr>
<td>in</td>
<td>Filter incoming routing updates</td>
<td>-</td>
</tr>
<tr>
<td>out</td>
<td>Filter outgoing routing updates</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

None
Usage
None

Examples
The following example filters all routes from RIP:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# distribute-list prefix 1 in
```

Related Commands
ip prefix-list

6.2.22 address-family

Command Purpose
Use the command enter Address Family command mode in router configuration mode.

Command Syntax

```
address-family ipv4 vrf WORD
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>VPN Routing/Forwarding instance name</td>
<td>Up to 15 characters</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration

Default
N/A

Usage
None

Examples
The following example shows how to enter Address Family command mode:

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# address-family ipv4
```

Related Commands
None
6.2.23 show ip protocol rip

Command Purpose

To show Routing Information Protocol (RIP), use the show ip protocol rip command in privileged EXEC mode.

Command Syntax

show ip protocol rip

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show ip rip interface command:

Switch# show ip protocol rip

Routing protocol is "rip"
    Sending updates every 30 seconds with +/-5 seconds
    Timeout after 180 seconds, Garbage collect after 120 seconds
    Outgoing update filter list for all interface is not set
    Incoming update filter list for all interface is not set
    Default redistribution metric is 1
    Redistributing:
        connected   metric default
    Default version control: send version 2, receive version 2

                   Interface    Send  Recv Key-chain
Routing for Networks:
    10.10.11.0/24
Routing Information Sources:
    Gateway Distance Last Update Bad Packets Bad Routes
Number of routes (including connected): 0
Distance: (default is 120)
Related Commands

None

6.2.24 debug rip

Command Purpose

Use this command to specify the options for the displayed debugging information for RIP events, RIP packets. Use the no parameter with this command to disable all debugging.

Command Syntax

default rip (all | events | PACKET | )
no debug rip (all | events | PACKET | )
no debug all ( rip | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>All RIP debug information</td>
<td>-</td>
</tr>
<tr>
<td>events</td>
<td>RIP events debug information is displayed</td>
<td>-</td>
</tr>
<tr>
<td>PACKET</td>
<td>packet (recv</td>
<td>send) (detail) Specifies RIP packets only</td>
</tr>
<tr>
<td>recv</td>
<td>Specifies that information for received packets be displayed</td>
<td>-</td>
</tr>
<tr>
<td>send</td>
<td>Specifies that information for sent packets be displayed</td>
<td>-</td>
</tr>
<tr>
<td>detail</td>
<td>Displays detailed information for the sent or received packet</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

Disabled

Usage

None

Examples

The following example displays information about the rip packets that are received and sent out from the connected router:

Switch# debug rip packet

Related Commands

show debugging rip
6.2.25  show debugging rip

Command Purpose

Use this command to display the RIP debugging status for these debugging options: nsm debugging, RIP event debugging, RIP packet debugging.

Command Syntax

show debugging rip

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show debugging rip command:

Switch# show debugging rip
RIP debugging status:
    RIP packet debugging is on

Related Commands

debug rip

6.2.26  show ip rip database database-summary

Command Purpose

Use this command to display the statistics for RIP routes.

Command Syntax

show ip rip database database-summary (vrf NAME | )
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf NAME</td>
<td>VPN Routing/Forwarding instance</td>
<td>Up to 15 characters</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP connected</td>
<td>1</td>
</tr>
<tr>
<td>RIP</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td>2</td>
</tr>
</tbody>
</table>
```

**Related Commands**

show ip rip database

**6.2.27 show resource rip**

**Command Purpose**

Use this command to display the route resources used by RIP protocol.

**Command Syntax**

show resource rip

**Command Mode**

Privileged EXEC
Default

None

Usage

None

Examples

The following is sample output from the show resource rip command:

```
Switch# show resource rip
RIP
Resource Used Capability
---------------------------------------------------------------
Routes 2 6144
```

Related Commands

show ip rip database

6.3 OSPF Commands

6.3.1 area authentication

Command Purpose

To enable authentication for an Open Shortest Path First (OSPF) area, use the area authentication command in router configuration mode. To remove an authentication specification of an area or a specified area from the configuration, use the no form of this command.

Command Syntax

area AREA-ID authentication (message-digest | )
no area AREA-ID authentication

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AREA-ID</td>
<td>Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address</td>
<td>IP address or number in the range of 0-4294967295</td>
</tr>
<tr>
<td>message-digest</td>
<td>(Optional) Enables Message Digest 5 (MD5) authentication on the area specified by the area-id argument</td>
<td>-</td>
</tr>
</tbody>
</table>
Command Mode

Router Configuration

Default

Type 0 authentication (no authentication)

Usage

Specifying authentication for an area sets the authentication to Type 1 (simple password) as specified in RFC 1247. If this command is not included in the configuration file, authentication of Type 0 (no authentication) is assumed.

The authentication type must be the same for all routers and access servers in an area. The authentication password for all OSPF routers on a network must be the same if they are to communicate with each other via OSPF. Use the `ip ospf authentication-key` interface command to specify this password.

If you enable MD5 authentication with the message-digest keyword, you must configure a password with the `ip ospf message-digest-key` interface command.

To remove the authentication specification for an area, use the `no` form of this command with the authentication keyword.

Examples

The following example mandates authentication for areas 0 and 10.0.0.0 of OSPF routing process 201. Authentication keys are also provided:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.251.201/24
Switch(config-if)# ip ospf authentication-key adcdedefgh
Switch(config)# interface eth-0-2
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.56.0.201/16
Switch(config-if)# ip ospf authentication-key ijklnmnop
Switch(config)# router ospf 201
Switch(config-router)# network 10.0.0.0 0.255.255.255 area 10.0.0.0
Switch(config-router)# network 192.168.0.0/16 area 0
Switch(config-router)# area 10.0.0.0 authentication
Switch(config-router)# area 0 authentication
```

Related Commands

`ip ospf authentication-key`
6.3.2 area default-cost

Command Purpose

To specify a cost for the default summary route sent into a stub, use the area default-cost command in router configuration mode. To remove the assigned default route cost, use the no form of this command.

Command Syntax

area AREA-ID default-cost COST
no area AREA-ID default-cost

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AREA-ID</td>
<td>Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address.</td>
<td>IP address or number in the range of 0-4294967295</td>
</tr>
<tr>
<td>COST</td>
<td>default cost value</td>
<td>0-16777214</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

COST: 1

Usage

The command is used only on an Area Border Router (ABR) attached to a stub.

There are two stub area router configuration commands: the stub and default-cost options of the area command. In all routers and access servers attached to the stub area, the area should be configured as a stub area using the stub option of the area command. Use the default-cost option only on an ABR attached to the stub area. The default-cost option provides the metric for the summary default route generated by the ABR into the stub area.

Examples

The following example shows how to configure a stub area and set its COST value:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.56.0.201/16
Switch(config)# router ospf 201
Switch(config-router)# network 10.0.0.0/8 area 10.0.0.0
Switch(config-router)# area 10.0.0.0 stub
Switch(config-router)# area 10.0.0.0 default-cost 20
Related Commands

None

6.3.3 area filter-list

Command Purpose

To filter prefixes advertised in type 3 link-state advertisements (LSAs) between Open Shortest Path First (OSPF) areas of an Area Border Router (ABR), use the area filter-list command in router configuration mode. To change or cancel the filter, use the no form of this command.

Command Syntax

area AREA-ID filter-list ( access ACCESSS-LIST-NAME | prefix PREFIX-LIST-NAME ) ( in | out )
no area AREA-ID filter-list ( access ACCESSS-LIST-NAME | prefix PREFIX-LIST-NAME ) ( in | out )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AREA-ID</td>
<td>Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address</td>
<td>IP address or number in the range of 0-4294967295</td>
</tr>
<tr>
<td>access</td>
<td>Indicates that an accesslist is used</td>
<td>-</td>
</tr>
<tr>
<td>ACCESSS-LIST-NAME</td>
<td>Name of an access list</td>
<td>A string with 1-20 characters</td>
</tr>
<tr>
<td>prefix</td>
<td>Indicates that a prefix list is used</td>
<td>-</td>
</tr>
<tr>
<td>PREFIX-LIST-NAME</td>
<td>Name of a prefix list</td>
<td>A string with 1-20 characters</td>
</tr>
<tr>
<td>in</td>
<td>Access list or prefix list applied to prefixes advertised to the specified area from other areas</td>
<td>-</td>
</tr>
<tr>
<td>out</td>
<td>Access list or prefix list applied to prefixes advertised out of the specified area to other areas</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

This command has no default behavior.

Usage

With this feature enabled in the “in” direction, all type 3 LSAs originated by the ABR to this area, based on information from all other areas, are filtered by the prefix list. Type 3 LSAs that were originated as a result of the area range command in another area are treated like any other type 3 LSA that was originated individually. Any prefix that does not match an entry in the prefix list is implicitly denied.
With this feature enabled in the “out” direction, all type 3 LSAs advertised by the ABR, based on information from this area to all other areas, are filtered by the prefix list. If the area range command has been configured for this area, type 3 LSAs that correspond to the area range are sent to all other areas, only if at least one prefix in the area range matches an entry in the prefix list.

If all specific prefixes are denied by the prefix list, type 3 LSAs that correspond to the area range command will not be sent to any other area. Prefixes that are not permitted by the prefix list are implicitly denied.

**Examples**

The following example filters prefixes that are sent from all other areas to area 1:

```
Switch# configure terminal
Switch(config)# router ospf 201
Switch(config-router)# area 1 filter-list prefix AREA_1 in
```

**Related Commands**

area range

**6.3.4 area range**

**Command Purpose**

To consolidate and summarize routes at an area boundary, use the area range command in router configuration mode. To disable this function, use the no form of this command.

**Command Syntax**

```
area AREA-ID range (ADDRESS MASK | ADDRESS / PREFIX-LENGTH) (advertise | not-advertise | )
no area AREA-ID range (ADDRESS MASK | ADDRESS / PREFIX-LENGTH )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AREA-ID</td>
<td>Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address</td>
<td>IP address or number in the range of 0-4294967295</td>
</tr>
<tr>
<td>ADDRESS</td>
<td>IPv4 address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PREFIX-LENGTH</td>
<td>Prefix length of the address</td>
<td>1-32</td>
</tr>
<tr>
<td>advertise</td>
<td>Advertise this range (default)</td>
<td>-</td>
</tr>
<tr>
<td>not-advertise</td>
<td>Do not advertise this range</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration

**Default**

This command is disabled by default.
Usage

The area range command is used only with Area Border Routers (ABRs). It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This behavior is called route summarization. Multiple area router configuration commands specifying the range option can be configured. Thus, OSPF can summarize addresses for many different sets of address ranges.

Examples

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 10.0.0.0 and for all hosts on network 192.168.110.0:

```plaintext
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.110.201/24
Switch(config)# interface eth-0-2
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.120.201/24
Switch(config)# interface eth-0-3
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.0/8
Switch(config)# router ospf 201
Switch(config-router)# network 192.168.110.0/24 area 0
Switch(config-router)# area 10.0.0.0 range 10.0.0.0/8
Switch(config-router)# area 0 range 192.168.110.0 255.255.0.0
```

Related Commands

None

6.3.5 area stub

Command Purpose

To define an area as a stub area, use the area stub command in router configuration mode. To disable this function, use the no form of this command.

Command Syntax

area AREA-ID stub ( no-summary | )
no area AREA-ID stub ( no-summary | )
### Command Mode

**Router Configuration**

### Default

No stub area is defined.

### Usage

You must configure the area stub command on all routers and access servers in the stub area. Use the area router configuration command with the default-cost keyword to specify the cost of a default internal router sent into a stub area by an ABR.

There are two stub area router configuration commands: the stub and default-cost options of the area router configuration command. In all routers attached to the stub area, the area should be configured as a stub area using the stub keyword of the area command. Use the default-cost keyword only on an ABR attached to the stub area. The default-cost keyword provides the metric for the summary default route generated by the ABR into the stub area.

To further reduce the number of link-state advertisements (LSAs) sent into a stub area, you can configure the no-summary keyword on the ABR to prevent it from sending summary LSAs (LSA type 3) into the stub area.

### Examples

The following example shows how to configure a stub area and set its COST value:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.56.0.201/16
Switch(config-if)# router ospf 201
Switch(config-router)# network 10.0.0.0/8 area 10.0.0.0
Switch(config-router)# area 10.0.0.0 stub
Switch(config-router)# area 10.0.0.0 default-cost 20
```

### Related Commands

None
6.3.6 area nssa

Command Purpose
To define an area as a NSSA area, use the area nssa command in router configuration mode. To disable this function, use the no form of this command.

Command Syntax
area AREA-ID nssa ( translator-role ( candidate | never | always ) ) ( no-summary | ) ( no-redistribution | ) ( default-information-originate ( metric METRIC_VALUE | metric-type TYPE-VALUE | ) )
no area AREA-ID nssa ( translator-role | ) ( no-summary | ) ( no-redistribution | ) ( default-information-originate | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AREA-ID</td>
<td>Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address</td>
<td>IP address or number in the range of 0-4294967295</td>
</tr>
<tr>
<td>candidate</td>
<td>(Optional) Configure the role for ABR in NSSA area as candidate for the translator router</td>
<td>-</td>
</tr>
<tr>
<td>never</td>
<td>(Optional) Configure the role for ABR in NSSA area as non-translator router</td>
<td>-</td>
</tr>
<tr>
<td>always</td>
<td>(Optional) Configure the role for ABR in NSSA area as the specified translator router</td>
<td>-</td>
</tr>
<tr>
<td>no-summary</td>
<td>(Optional) Prevents an Area Border Router (ABR) from sending Summary LSAs into the NSSA area</td>
<td>-</td>
</tr>
<tr>
<td>no-redistribution</td>
<td>(Optional) Prevents an Area Border Router (ABR) from importing routes into the NSSA area</td>
<td>-</td>
</tr>
<tr>
<td>default-information-originate</td>
<td>(Optional) Configure an ASBR to send default type 7 LSA into the NSSA area</td>
<td>-</td>
</tr>
<tr>
<td>metric METRIC_VALUE</td>
<td>(Optional) Configure metric for the default originate route</td>
<td>0-16777214</td>
</tr>
<tr>
<td>metric-type TYPE-VALUE</td>
<td>(Optional) Configure metric type for the default originate route</td>
<td>1-2</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration

Default
No NSSA area is defined.

Usage
No NSSA area is configured as default. You must configure the area nssa command on all routers and access servers in the NSSA area.
There are many similarities between NSSA and stub area, neither of which propagates external routes from other area. The difference is that NSSA area can introduce and propagate external routes to the OSPF autonomous domain, while STUB area can not introduce external routes.
Examples

The following example shows how to configure a NSSA area:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.56.0.201/16
Switch(config-if)# router ospf 201
Switch(config-router)# network 10.0.0.0/8 area 10.0.0.0
Switch(config-router)# area 10.0.0.0 nssa

Related Commands

None

6.3.7  auto-cost

Command Purpose

To control how Open Shortest Path First (OSPF) calculates default metrics for the interface, use the auto-cost command in router configuration mode. To assign cost based only on the interface type, use the no form of this command.

Command Syntax

auto-cost reference-bandwidth RATE
no auto-cost reference-bandwidth

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RATE</td>
<td>Rate in Mbps (bandwidth).</td>
<td>1-4294967</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

100 Mbps

Usage

The value set by the ip ospf cost command overrides the cost resulting from the auto-cost command. Bandwidth dividing port rate is cost.

Examples

The following example changes the cost of the cost link to 1Gbps:

Switch# configure terminal
Switch(config)# router ospf 1
Switch(config-router)# auto-cost reference-bandwidth 1000

Related Commands

ip ospf cost
### 6.3.8 clear ip ospf

#### Command Purpose

To clear redistribution based on the Open Shortest Path First (OSPF) routing process ID, use the clear ip ospf command in privileged EXEC mode.

#### Command Syntax

```
clear ip ospf [PID] process
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PID</td>
<td>(Optional) Process ID</td>
<td>0-65535</td>
</tr>
</tbody>
</table>

#### Command Mode

Privileged EXEC

#### Default

None

#### Usage

Use the PID argument to clear only one OSPF process. If the PID argument is not specified, all OSPF processes are cleared.

#### Examples

The following example clears all OSPF processes:

```
Switch# clear ip ospf process
```

#### Related Commands

None

### 6.3.9 compatible rfc1583

#### Command Purpose

To restore the method used to calculate summary route costs per RFC 1583, use the compatible rfc1583 command in router configuration mode. To disable RFC 1583 compatibility, use the no form of this command.

#### Command Syntax

```
compatible rfc1583
no compatible rfc1583
```
Command Mode
Router Configuration

Default
Not compatible with RFC 1583.

Usage
To minimize the chance of routing loops, all Open Shortest Path First (OSPF) routers in an OSPF routing domain should have RFC compatibility set identically. Because of the introduction of RFC 2328, OSPF Version 2, the method used to calculate summary route costs has changed. Use the no compatible rfc1583 command to enable the calculation method used per RFC 2328.

Examples
The following example specifies that the router process is compatible with RFC 1583:

Switch# configure terminal
Switch(config)# router ospf 1
Switch(config-router)# compatible rfc1583

Related Commands
None

6.3.10 default-information originate (OSPF)

Command Purpose
To generate a default external route into an Open Shortest Path First (OSPF) routing domain, use the default-information originate command in router configuration mode. To disable this feature, use the no form of this command.

Command Syntax
default-information originate ( route-map WORD | always | metric METRIC-VALUE | metric-type TYPE-VALUE )
no default-information originate ( route-map WORD | always | metric | metric-type )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>always</td>
<td>(Optional) Always advertises the default route regardless of whether the system has a default route</td>
<td>-</td>
</tr>
<tr>
<td>metric METRIC-VALUE</td>
<td>metric-value (Optional) Metric used for generating the default route. If you omit a value and do not specify a value using the default-metric router configuration command, the default metric value is 1.</td>
<td>0-16777214</td>
</tr>
<tr>
<td>metric-type TYPE-VALUE</td>
<td>(Optional) External link type associated with the default route advertised into the OSPF routing domain. It can be type 1 or type 2 LSA</td>
<td>1-2</td>
</tr>
<tr>
<td>route-map WORD</td>
<td>Route map reference</td>
<td>A string with 1-20 characters</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration
Default

This command is disabled by default.

Usage

Whenever you use the redistribute or the default-information router configuration command to redistribute routes into an OSPF routing domain, the switch automatically becomes an autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a default route into the OSPF routing domain. The system still must have a default route for itself before it generates one, except when you have specified the always keyword.

Examples

The following example specifies a metric for the default route redistributed into the OSPF routing domain and an external metric type:

```
Switch# configure terminal
Switch(config)# router ospf 109
Switch(config-router)# redistribute rip metric 100
Switch(config-router)# default-information originate metric 100 metric-type 1
```

Related Commands

redistribute (OSPF)

6.3.11 default-metric (OSPF)

Command Purpose

To set default metric values for the Open Shortest Path First (OSPF) routing protocol, use the default-metric command in router configuration mode. To return to the default state, use the no form of this command.

Command Syntax

```
default-metric METRIC-VALUE
no default-metric (METRIC-VALUE | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>METRIC-VALUE</td>
<td>Default metric value appropriate for the specified routing protocol.</td>
<td>0-16777214</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

20
Usage

The default-metric command is used in conjunction with the redistribute router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes.

Examples

The example advertises OSPF-derived routes using RIP and assigns the Internal Gateway Protocol (IGP)-derived routes a RIP metric of 10.:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# default-metric 10
Switch(config-router)# redistribute rip
```

Related Commands

redistribute (OSPF)

6.3.12 distance (OSPF)

Command Purpose

To define Open Shortest Path First (OSPF) route administrative distances based on route type, use the distance command in router configuration mode. To restore the default value, use the no form of this command.

Command Syntax

distance { DISTANCE | ospf [ external DIST1 ] [ inter-area DIST2 ] [ intra-area DIST3 ] }  
no distance { DISTANCE | ospf }

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISTANCE</td>
<td>Administrative distance. An integer from 1 to 255. (Routes with a distance value of 255 are not installed in the routing table.)</td>
<td>1-255</td>
</tr>
<tr>
<td>external DIST1</td>
<td>(Optional) Sets the distance for routes from other routing domains, learned by redistribution. Range is 1 to 255.</td>
<td>1-255</td>
</tr>
<tr>
<td>inter-area DIST2</td>
<td>(Optional) Sets the distance for all routes from one area to another area. Range is 1 to 255.</td>
<td>1-255</td>
</tr>
<tr>
<td>intra-area DIST3</td>
<td>(Optional) Sets the distance for all routes within an area. Range is 1 to 255.</td>
<td>1-255</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration
Default

DIST1: 110
DIST2: 110
DIST3: 110

Usage

You may specify one of the keywords or use distance only to apply to all types of routes.
The distance command allows you to set a distance for an entire group of routes, rather than a specific route that passes an access list.
A common reason to use the distance command is when you have multiple OSPF processes with mutual redistribution, and you want to prefer internal routes from one over external routes from the other.

Examples

The example advertises OSPF-derived routes using RIP and assigns the Internal Gateway Protocol (IGP)-derived routes a RIP distance of 90:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# distance 90
Switch(config-router)# redistribute rip
```

Related Commands

None

6.3.13 distribute-list (OSPF)

Command Purpose

To filter networks received in updates or suppress networks from being advertised in updates, use the distribute-list command in router configuration mode. To cancel this function, use the no form of this command.

Command Syntax

```
distribute-list ACCESSS-LIST-NAME ( in | out )
no distribute-list ACCESSS-LIST-NAME ( in | out )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCESSS-LIST-NAME</td>
<td>Name of an access list to be applied</td>
<td>A string with 1-20 characters</td>
</tr>
<tr>
<td>in</td>
<td>Filter networks received in updates</td>
<td>-</td>
</tr>
<tr>
<td>out</td>
<td>Suppress networks from being advertised in updates</td>
<td>-</td>
</tr>
</tbody>
</table>
Command Mode

Router Configuration

Default

None

Usage

This command must specify an access list.

Examples

In the following example, OSPF process 1 is configured to accept two networks, network 20.0.0.0 and network 10.108.0.0:

```
Switch# configure terminal
Switch(config)# ip access-list acl1
Switch(config-ip-acl)# permit any 20.0.0.0 0.0.255.255 any
Switch(config-ip-acl)# permit any 10.108.0.0 0.0.255.255 any
Switch(config-ip-acl)# deny any any
Switch(config)# router ospf 1
Switch(config-router)# network 10.108.0.0/16 area 1
Switch(config-router)# distribute-list acl1 in
```

Related Commands

ip access-list

6.3.14 ip ospf authentication

Command Purpose

To specify the authentication type for an interface, use the ip ospf authentication command in interface configuration mode. To remove the authentication type for an interface, use the no form of this command.

Command Syntax

```
ip ospf authentication (message-digest | null | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>message-digest</td>
<td>(Optional) Specifies that message-digest authentication will be used</td>
<td>-</td>
</tr>
<tr>
<td>null</td>
<td>(Optional) No authentication is used. Useful for overriding password or message-digest authentication if configured for an area</td>
<td>-</td>
</tr>
</tbody>
</table>
Command Mode
Interface Configuration

Default
The area default is no authentication (null authentication).

Usage
Before using the ip ospf authentication command, configure a password for the interface using the ip ospf authentication-key command. If you use the ip ospf authentication message-digest command, configure the message-digest key for the interface with the ip ospf message-digest-key command.

Examples
The following example enables message-digest authentication:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ip ospf authentication message-digest

Related Commands
area authentication
ip ospf authentication-key
ip ospf message-digest-key

6.3.15 ip ospf authentication-key

Command Purpose
To assign a password to be used by neighboring routers that are using the Open Shortest Path First (OSPF) simple password authentication, use the ip ospf authentication-key command in interface configuration mode. To remove a previously assigned OSPF password, use the no form of this command.

Command Syntax
ip ospf authentication-key (8 | ) PASSWORD
no ip ospf authentication-key

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PASSWORD</td>
<td>Any continuous printable string of characters that can be entered from the keyboard up to 8 bytes in length</td>
<td>A string with 8 characters</td>
</tr>
<tr>
<td>(8)</td>
<td>Specifies a hidden password will follow</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
No password is specified.
Usage

The password created by this command is used as a “key” that is inserted directly into the OSPF header when the switch originates routing protocol packets. A separate password can be assigned to each network on a per-interface basis. All neighboring routers on the same network must have the same password to be able to exchange OSPF information.

Examples

The following example enables the authentication key with the string yourpass:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf authentication-key yourpass

The following example enables the authentication key with the encrypt password 91c38996a1aa5699:

Switch# configure terminal
Switch(config)# interface eth-0-2
Switch(config-if)# no switchport
Switch(config-if)# ip ospf authentication-key 8 91c38996a1aa5699

Related Commands

area authentication
ip ospf authentication

6.3.16 ip ospf cost

Command Purpose

To explicitly specify the cost of sending a packet on an interface, use the ip ospf cost command in interface configuration mode. To reset the path cost to the default value, use the no form of this command.

Command Syntax

ip ospf cost INTERFACE-COST
no ip ospf cost

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERFACE-COST</td>
<td>The cost of sending a packet on an interface</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration
Default

Different port rate has different default cost.

Usage

You can set the metric manually using this command, if you need to change the default. Using the bandwidth command changes the link cost as long as this command is not used.

Examples

The following example sets the interface cost value to 65:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf cost 65
```

Related Commands

auto-cost reference bandwidth

6.3.17 ip ospf database-filter all out

Command Purpose

To filter outgoing link-state advertisements (LSAs) to an Open Shortest Path First (OSPF) interface, use the ip ospf database-filter all out command in interface configuration mode. To restore the forwarding of LSAs to the interface, use the no form of this command.

Command Syntax

```
ip ospf database-filter all out
no ip ospf database-filter
```

Command Mode

Interface Configuration

Default

This command is disabled by default. All outgoing LSAs are flooded to the interface.
Usage

OSPF floods new LSAs over all interfaces in an area, except the interface on which the LSA arrives. This redundancy ensures robust flooding. However, too much redundancy can waste bandwidth and might lead to excessive link and CPU usage in certain topologies, resulting in destabilizing the network. To avoid this, use the database-filter command to block flooding of LSAs over specified interfaces.

Examples

The following example prevents flooding of OSPF LSAs to broadcast, nonbroadcast, or point-to-point networks reachable through the interface eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf database-filter all out
```

Related Commands

None

6.3.18  ip ospf dead-interval

Command Purpose

To set the interval during which at least one hello packet must be received from a neighbor before the router declares that neighbor down, use the ip ospf dead-interval command in interface configuration mode. To restore the default value, use the no form of this command.

Command Syntax

```
ip ospf dead-interval SECONDS
no ip ospf dead-interval
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>The interval during which at least one hello packet must be received from a neighbor before the router declares that neighbor down. The value must be the same for all nodes on the network</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

SECONDS: The neighbor is been considered as dead in 40s by default.
Usage

The dead interval is advertised in OSPF hello packets. This value must be the same for all networking devices on a specific network. Specifying a smaller dead interval (seconds) will give faster detection of a neighbor being down and improve convergence, but might cause more routing instability.

Examples

The following example sets the OSPF dead interval to 20 seconds:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf dead-interval 20
```

Related Commands

`ip ospf hello-interval`
`show ip ospf interface`

6.3.19 `ip ospf hello-interval`

Command Purpose

To specify the interval between hello packets that the switch sends on the interface, use the `ip ospf hello-interval` command in interface configuration mode. To return to the default time, use the no form of this command.

Command Syntax

```
ip ospf hello-interval SECONDS
no ip ospf hello-interval
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>Interval (in seconds) during which the router must receive at least one hello packet from a neighbor or else that neighbor is removed from the peer list and does not participate in routing. The range is 1 to 65535. The value must be the same for all nodes on the network</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

10 seconds (Ethernet)
30 seconds (non-broadcast)
Usage

This value is advertised in the hello packets. The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

Examples

The following example sets the interval between hello packets to 15 seconds:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf hello-interval 15
```

Related Commands

ip ospf dead-interval

6.3.20  ip ospf message-digest-key md5

Command Purpose

To enable Open Shortest Path First (OSPF) Message Digest 5 (MD5) authentication, use the ip ospf message-digest-key command in interface configuration mode. To remove an old MD5 key, use the no form of this command.

Command Syntax

```
ip ospf message-digest-key KEY-ID md5 (8 | ) KEY
no ip ospf message-digest-key KEY-ID
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEY-ID</td>
<td>An identifier in the range from 1 to 255</td>
<td>1-255</td>
</tr>
<tr>
<td>(8)</td>
<td>Specifies a hidden password will follow</td>
<td>-</td>
</tr>
<tr>
<td>KEY</td>
<td>Alphanumeric password of up to 16 bytes</td>
<td>A string with 1-16 characters</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

OSPF MD5 authentication is disabled.
Usage

All routers access the same network/sub network share the same password when using this type of authentication. For every OSPF packet, the password is used for generating/examining the “message digest” which is at the tail of the OSPF packet. This “message digest” is processed by OSPF packet and password. There may multiple passwords be activated on the same interface, this command line always used to transit smoothly to the new password from the old one.

Examples

The following example sets a new key 19 with the password 8ry4222:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf message-digest-key 10 md5 xvv560qle
Switch(config-if)# ip ospf message-digest-key 19 md5 8ry4222
```

The following example sets a new key 2 with the encrypt password 91c38996a1aa5699:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf message-digest-key 2 md5 8 91c38996a1aa5699
```

Related Commands

area authentication
service password-encryption
ip ospf authentication

6.3.21 ip ospf mtu

Command Purpose

To set the MTU value when sending Database Descriptor (DD) packets, use the ip ospf mtu command in interface configuration mode. To restore a default value, use the no form of this command.

Command Syntax

```
ip ospf mtu MTU-VALUE
no ip ospf mtu
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTU-VALUE</td>
<td>MTU value</td>
<td>576-65535</td>
</tr>
</tbody>
</table>
Command Mode

Interface Configuration

Default

1500

Usage

Whenever OSPF constructs packets, it uses interface MTU size as Maximum IP packet size. This command forces OSPF to use the specified value overriding the actual interface MTU size.

This command allows an administrator to configure the MTU size recognized by the OSPF protocol. It does not configure the MTU settings on the kernel. OSPF will not recognize MTU size configuration changes made to the kernel until the MTU size is updated through the CLI.

Examples

The following example sets a new MTU value when sending OSPF DD packets:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf mtu 1280

Related Commands

ip ospf mtu-ignore

6.3.22 ip ospf mtu-ignore

Command Purpose

To disable Open Shortest Path First (OSPF) maximum transmission unit (MTU) mismatch detection on receiving Database Descriptor (DD) packets, use the ip ospf mtu-ignore command in interface configuration mode. To reset to default, use the no form of this command.

Command Syntax

ip ospf mtu-ignore
no ip ospf mtu-ignore

Command Mode

Interface Configuration
Default

OSPF MTU mismatch detection is enabled.

Usage

OSPF checks whether neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange DD packets. If the receiving MTU in the DD packet is higher than the IP MTU configured on the incoming interface, OSPF adjacency will not be established.

Examples

The following example disables MTU mismatch detection on receiving DD packets:

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

Related Commands

ip ospf mtu

6.3.23  ip ospf priority

Command Purpose

To set the router priority, which helps determine the designated router for this network, use the ip ospf priority command in interface configuration mode. To return to the default value, use the no form of this command.

Command Syntax

```
ip ospf priority NUMBER-VALUE
no ip ospf priority
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER-VALUE</td>
<td>A number value that specifies the priority of the router.</td>
<td>0-255</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

Priority of 1
Usage

When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the designated router or backup designated router. Router priority is configured only for interfaces to multi-access networks (in other words, not to point-to-point networks). This priority value is used when you configure Open Shortest Path First (OSPF) for non-broadcast networks using the neighbor router configuration command for OSPF.

Examples

The following example sets the router priority value to 4:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf priority 4
```

Related Commands

- `ip ospf network`
- `neighbor (OSPF)`

6.3.24 ip ospf retransmit-interval

Command Purpose

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface, use the `ip ospf retransmit-interval` command in interface configuration mode. To return to the default value, use the `no` form of this command.

Command Syntax

```
ip ospf retransmit-interval SECONDS
no ip ospf retransmit-interval
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>Time (in seconds) between retransmissions. The default is 5 seconds</td>
<td>1-65535 seconds</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

5 seconds
Usage

When a router sends an LSA to its neighbor, it keeps the LSA until it receives back the acknowledgment message. If the router receives no acknowledgment, it will resend the LSA. The setting of this parameter should be conservative, or needless retransmission will result. The value should be larger for serial lines and virtual links.

Examples

The following example sets the retransmit interval value:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf retransmit-interval 8
```

Related Commands

None

6.3.25 ip ospf transmit-delay

Command Purpose

To set the estimated time required to send a link-state update packet on the interface, use the ip ospf transmit-delay command in interface configuration mode. To return to the default value, use the no form of this command.

Command Syntax

```
ip ospf transmit-delay SECONDS
no ip ospf transmit-delay
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>Time (in seconds) between retransmissions. The default is 5 seconds</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

1 second

Usage

Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the seconds argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface.
If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low-speed links.

**Examples**

The following example sets the retransmit delay value to 3 seconds:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf transmit-delay 3
```

**Related Commands**

None

6.3.26 **ip ospf network**

**Command Purpose**

To configure the Open shortest path first (OSPF) network type to a type other than the default for a given medium, use the `ip ospf network` command in interface configuration mode. To return to the default value, use the no form of this command.

**Command Syntax**

```
ip ospf network ( broadcast | non-broadcast | point-to-multipoint [ non-broadcast ] | point-to-point )
no ip ospf network
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>broadcast</td>
<td>Sets the network type to broadcast. (Such as Ethernet, FDDI)</td>
<td>-</td>
</tr>
<tr>
<td>non-broadcast</td>
<td>Sets the network type to non-broadcast multi-access (NBMA)</td>
<td>-</td>
</tr>
<tr>
<td>point-to-multipoint</td>
<td>Sets the network type to point-to-multipoint.</td>
<td>-</td>
</tr>
<tr>
<td>point-to-point</td>
<td>Sets the network type to point-to-point</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

Depends on the network type.
Usage

Using this feature, you can configure broadcast networks as NBMA networks when, for example, routers in your network do not support multicast addressing. You can also configure non-broadcast multi-access networks as broadcast networks. This feature saves you from needing to configure neighbors.

Configuring NBMA networks as either broadcast or non-broadcast assumes that there are virtual circuits from every router to every router or fully meshed networks. However, there are other configurations where this assumption is not true. For example, a partially meshed network. In these cases, you can configure the OSPF network type as a point-to-multipoint network. Routing between two routers that are not directly connected will go through the router that has virtual circuits to both routers. You need not configure neighbors when using this feature.

If this command is issued on an interface that does not allow it, this command will be ignored.

OSPF has two features related to point-to-multipoint networks. One feature applies to broadcast networks; the other feature applies to non-broadcast networks:

On point-to-multipoint, broadcast networks, you can use the neighbor command, and you must specify a cost to that neighbor.

On point-to-multipoint, non-broadcast networks, you must use the neighbor command to identify neighbors. Assigning a cost to a neighbor is optional.

Examples

The following example sets your OSPF network as a non-broadcast network:

```bash
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.77.17/24
Switch(config-if)# ip ospf network non-broadcast
```

Related Commands

Neighbor (OSPF)

6.3.27 neighbor (OSPF)

Command Purpose

To configure Open Shortest Path First (OSPF) routers interconnecting to non-broadcast networks, use the neighbor command in router configuration mode. To remove a configuration, use the no form of this command.

Command Syntax

```bash
neighbor IP_ADDR { priority NUMBER | poll-interval SECONDS }
neighbor IP_ADDR { cost COST | }
no neighbor IP_ADDR { priority NUMBER | poll-interval SECONDS }
```
no neighbor IP_ADDR ( cost COST | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>Interface IP address of the neighbor</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>priority NUMBER</td>
<td>(Optional) A number that indicates the router priority value of the non-broadcast neighbor associated with the IP address specified. The default is 0. This keyword does not apply to point-to-multipoint interfaces</td>
<td>0-255</td>
</tr>
<tr>
<td>poll-interval SECONDS</td>
<td>(Optional) A number value that represents the poll interval time (in seconds). RFC 1247 recommends that this value be much larger than the hello interval. The default is 120 seconds (2 minutes). This keyword does not apply to point-to-multipoint interfaces.</td>
<td>1-65535 seconds</td>
</tr>
<tr>
<td>cost COST</td>
<td>(Optional) Assigns a cost to the neighbor, in the form of an integer from 1 to 65535. Neighbors with no specific cost configured will assume the cost of the interface, based on the ip ospf cost command. For point-to-multipoint interfaces, the cost keyword and the number argument are the only options that are applicable. This keyword does not apply to non-broadcast multi-access (NBMA) networks</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration

**Default**

No configuration is specified.

**Usage**

One neighbor entry must be included in the switch configuration for each known non-broadcast network neighbor. The neighbor address must be the primary address of the interface.

If a neighboring router has become inactive (hello packets have not been received for the Router Dead Interval period), it may still be necessary to send hello packets to the dead neighbor. These hello packets will be sent at a reduced rate called Poll Interval.

When the router first starts up, it sends only hello packets to those routers with nonzero priority, that is, routers that are eligible to become designated routers (DRs) and backup designated routers (BDRs). After the DR and BDR are selected, DR and BDR will then start sending hello packets to all neighbors in order to form adjacencies.

**Examples**

The following example declares a router at address 192.168.3.4 on a non-broadcast network, with a priority of 1 and a poll interval of 180 seconds:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# neighbor 192.168.3.4 priority 1 poll-interval 180
```

**Related Commands**

`ip ospf priority`
6.3.28 network area (OSPF)

Command Purpose

To define the interfaces on which Open Shortest Path First (OSPF) runs and to define the area ID for those interfaces, use the network area command in router configuration mode. To disable OSPF routing for interfaces defined with the address wildcard-mask pair, use the no form of this command.

Command Syntax

```
network { IP_ADDR WILDCARD-MASK | IP-ADDRESS/PREFIX-LENGTH } area AREA-ID
no network { IP-ADDRESS WILDCARD-MASK | IP-ADDRESS/PREFIX-LENGTH } area AREA-ID
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>Interface IP address of the neighbor</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>WILDCARD-MASK</td>
<td>IP-address-type mask that includes “don't care” bits</td>
<td>IPv4 mask</td>
</tr>
<tr>
<td>PREFIX-LENGTH</td>
<td>Prefix length for the network</td>
<td>1-32</td>
</tr>
<tr>
<td>AREA-ID</td>
<td>Area that is to be associated with the OSPF address range. It can be specified as either a decimal value or as an IP address</td>
<td>IP address or number in the range of 0-4294967295</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

This command is disabled by default.

Usage

The IP-ADDRESS and WILDCARD-MASK arguments together allow you to define one or multiple interfaces to be associated with a specific OSPF area using a single command.

Examples

The following partial example initializes OSPF routing process 109, and defines four OSPF areas 10.9.50.0, 2, 3, and 0. Areas 10.9.50.0, 2, and 3 mask specific address ranges, and area 0 enables OSPF for all other networks:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.108.20.1/24
Switch(config)# router ospf 109
Switch(config-router)# network 10.108.20.0/24 area 10.9.50.0
Switch(config-router)# network 10.108.0.0/16 area 2
```
Switch(config-router)# network 10.109.10.0/24  area 3
Switch(config-router)# network 0.0.0.0/0  area 0

Related Commands

router ospf

6.3.29 overflow database external

Command Purpose

Use this command to configure the size of the external database and the time the router waits before its entries to exit the overflow state. Use the no parameter with this command to revert to default.

Command Syntax

overflow database external MAXLSAS RECOVERTIME
no overflow database external

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAXLSAS</td>
<td>The maximum number of LSAs. Note that this value should be the same</td>
<td>0-2147483647</td>
</tr>
<tr>
<td>RECOVERTIME</td>
<td>The number of seconds the router waits before trying to exit the database</td>
<td>0-65535</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

None.

Usage

Use this command to limit the number of AS-external-LSAs a router can receive, once it is in the wait state. It takes the number of seconds specified as the RECOVERTIME to recover from this state.

Examples

The following example shows setting the maximum number of LSAs and the time to recover from overflow state:

Switch# configure terminal
Switch(config)# router ospf 200
Switch(config-router)# network 10.108.0.0/16 area 0
Switch(config-router)# overflow database external 5 3
Related Commands

router ospf

6.3.30 passive-interface (OSPF)

Command Purpose

To disable sending routing updates for the Open Shortest Path First (OSPF) on an interface, use the passive-interface command in router configuration mode. To re-enable the sending of routing updates, use the no form of this command.

Command Syntax

passive-interface IFNAME
no passive-interface IFNAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>The interface name</td>
<td>Support physical/aggregation/loopback/tunnel/vlan interfaces</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

Routing updates are sent on the interface.

Usage

If you disable the sending of routing updates on an interface, the particular subnet will continue to be advertised to other interfaces, and updates from other switches on that interface continue to be received and processed.

Examples

The following example sets the interface eth-0-1 as passive:

Switch# configure terminal
Switch(config)# router ospf 200
Switch(config-router)# network 10.108.0.0/16 area 0
Switch(config-router)# passive-interface eth-0-1

Related Commands

router ospf
6.3.31 redistribute (OSPF)

Command Purpose
To redistribute routes from one routing domain into Open Shortest Path First (OSPF) routing domain, use the redistribute command in router configuration mode. To disable redistribution, use the no form of this command.

Command Syntax
redistribute PROTOCOL [ route-map WORD ] [ tag TAG-VALUE ] [ metric METRIC-VALUE ] [ metric-type TYPE-VALUE ]
no redistribute PROTOCOL [ metric METRIC-VALUE ] [ metric-type TYPE-VALUE ]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-map WORD</td>
<td>Route map reference.</td>
<td>A string with 1-20 characters</td>
</tr>
<tr>
<td>PROTOCOL</td>
<td>(Optional) The name of a routing protocol, or the keyword connected, or static. If you specify a routing protocol</td>
<td>use one of the following keywords: static, connected, bgp, and rip</td>
</tr>
<tr>
<td>tag TAG-VALUE</td>
<td>Set tag for routes redistributed into OSPF</td>
<td>0-4294967295</td>
</tr>
<tr>
<td>metric METRIC-VALUE</td>
<td>(Optional) When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified</td>
<td>0-16777214</td>
</tr>
<tr>
<td>metric-type TYPE-VALUE</td>
<td>For OSPF, the external link type associated with the default route advertised into the OSPF routing domain. It can be one of two values</td>
<td>1-2</td>
</tr>
</tbody>
</table>

Command Mod
Router Configuration

Default
Route redistribution is disabled.
metric metric-value: 20
metric-type TYPE-VALUE: Type 2 external route

Usage
The metric value specified in the redistribute command supersedes the metric value specified using the default-metric command.

Examples
The following example redistribute the static routes into OSPF with metric 10:
Switch# configure terminal
Switch(config)# router ospf 119
Switch(config-router)# network 10.108.0.0/16 area 100
Switch(config-router)# redistribute static metric 10

Related Commands
default-metric
6.3.32  router-id (OSPF)

Command Purpose

To use a fixed router ID, use the router-id command in router configuration mode. To force Open Shortest Path First (OSPF) to use the previous OSPF router ID behavior, use the no form of this command.

Command Syntax

router-id IP_ADDR
no router-id

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>Router ID in IP address format</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

No OSPF routing process is defined.

Usage

You can configure an arbitrary value in the IP address format for each router. However, each router ID must be unique.

If this command is used on an OSPF router process which is already active (has neighbors), the new router-ID is used at the next reload or at a manual OSPF process restart. To manually restart the OSPF process, use the clear ip ospf command.

Examples

The following example specifies a fixed router-id:

Switch# configure terminal
Switch(config)# router ospf 119
Switch(config-router)# router-id 10.1.1.1

Related Commands

clear ip ospf
router ospf
6.3.33 router ospf

Command Purpose

To configure an Open Shortest Path First (OSPF) routing process, use the router ospf command in global configuration mode. To terminate an OSPF routing process, use the no form of this command.

Command Syntax

```
router ospf [ PROCESS-ID [ vrf VPN-NAME ] ]
```

```
no router ospf [ PROCESS-ID ]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROCESS-ID</td>
<td>Internally used identification parameter for an OSPF routing process. If you don't assign a PROCESS-ID, it enter process ID 0. Process ID 0 will be closed if you use the no form of this command and don't assign PROCESS-ID.</td>
<td>1-65535</td>
</tr>
<tr>
<td>vrf VPN-NAME</td>
<td>(Optional) Specifies the name of the VPN routing and forwarding (VRF) instance to associate with OSPF VRF processes</td>
<td>A string with 1-15 characters</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

No OSPF routing process is defined.

Usage

You can specify multiple OSPF routing processes in each router. If you do not specify the process-id, the process-id will be the default 0.

Examples

The following example configures an OSPF routing process and assign a process number of 109:

```
Switch# configure terminal
Switch(config)# router ospf 109
Switch(config-router)#
```

Related Commands

network area
6.3.34 summary-address (OSPF)

Command Purpose

To create aggregate addresses for Open Shortest Path First (OSPF), use the summary-address command in router configuration mode. To restore the default, use the no form of this command.

Command Syntax

```
summary-address PREFIX/PREFIX-LENGTH (not-advertise | tag TAG-VALUE | )
no summary-address PREFIX/PREFIX-LENGTH (not-advertise | tag TAG-VALUE | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PREFIX</td>
<td>IP route prefix for the destination</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PREFIX-LENGTH</td>
<td>Prefix length for the network</td>
<td>1-32</td>
</tr>
<tr>
<td>not-advertise</td>
<td>(Optional) Suppress routes that match the specified prefix/mask pair. This keyword</td>
<td></td>
</tr>
<tr>
<td></td>
<td>applies to OSPF only</td>
<td></td>
</tr>
<tr>
<td>tag TAG-VALUE</td>
<td>Route tag value. The default tag is 0.</td>
<td>0-4294967295</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

This command is disabled by default.

Usage

Routes learned from other routing protocols can be summarized. The metric used to advertise the summary is the largest metric of all the more specific routes. This command helps reduce the size of the routing table.

Using this command for OSPF causes an OSPF Autonomous System Boundary Router (ASBR) to advertise one external route as an aggregate for all redistributed routes that are covered by the address. For OSPF, this command summarizes only routes from other routing protocols that are being redistributed into OSPF. Use the area range command for route summarization between OSPF areas.

OSPF does not support the summary-address 0.0.0.0/0 command.

Examples

In the following example, the summary address 10.1.0.0 includes address 10.1.1.0, 10.1.2.0, 10.1.3.0, and so on. Only the address 10.1.0.0 is advertised in an external link-state advertisement:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# summary-address 10.1.0.0/16
```
Related Commands

area range

6.3.35 show ip ospf

Command Purpose

To display general information about Open Shortest Path First (OSPF) routing processes, use the show ip ospf command in user EXEC or privileged EXEC mode.

Command Syntax

show ip ospf (PROCESS-ID | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROCESS-ID</td>
<td>Internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process</td>
<td>0-65535</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show ip ospf command:

Switch# show ip ospf

Routing Process "ospf 100" with ID 11.11.11.11
Process uptime is 0 minute
Process bound to VRF default
Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPF's 10 secs
Refresh timer 10 secs
Number of incoming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 0. Checksum 0x0000000
Number of opaque AS LSA 0. Checksum 0x0000000
Number of non-default external LSA 0
External LSA database is unlimited.
Number of LSA originated 1
Number of LSA received 3
Number of areas attached to this router: 1
  Area 1
    Number of interfaces in this area is 1(1)
    Number of fully adjacent neighbors in this area is 1
    Number of fully adjacent virtual neighbors through this area is 0
    Area has no authentication
    SPF algorithm last executed 00:00:38.995 ago
    SPF algorithm executed 1 times
    Number of LSA 4. Checksum 0x0235ff

Related Commands
None

6.3.36 show ip ospf border-routers

Command Purpose
To display the internal Open Shortest Path First (OSPF) routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the show ip ospf border-routers command in privileged EXEC mode.

Command Syntax
show ip ospf border-routers

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following is sample output from the show ip ospf border-routers command:
Switch# show ip ospf border-routers
OSPF process 100 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 22.22.22.22 [1] via 172.10.1.2, eth-0-10, ABR, Area 1

Related Commands
None

6.3.37 show ip ospf database

Command Purpose
To display lists of information related to the Open Shortest Path First (OSPF) database for a specific router, use the show ip ospf database command in EXEC mode.

Command Syntax
show ip ospf (PROCESS-ID | ) database database-summary
show ip ospf (PROCESS-ID | ) database (self-originate | max-age | adv-router IP_ADDR )
show ip ospf (PROCESS-ID | ) database (asbr-summary | external | network | router | summary | nssa-external | opaque-link | opaque-area | opaque-as ) (self-originate | adv-router IP_ADDR )
show ip ospf (PROCESS-ID | ) database (asbr-summary | external | network | router | summary | nssa-external | opaque-link | opaque-area | opaque-as ) LINK-STATE-ID (self-originate | adv-router A.B.C.D | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROCESS-ID</td>
<td>Internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process</td>
<td>1-65535</td>
</tr>
<tr>
<td>adv-router IP_ADDR</td>
<td>(Optional) Displays all the LSAs of the specified router. If no IP address is included, the information is about the local router itself (in this case, the same as self-originate)</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>LINK-STATE-ID</td>
<td>(Optional) Portion of the Internet environment that is being described by the advertisement. The value entered depends on the advertisement's LS type. It must be entered in the form of an IP address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>asbr-summary</td>
<td>(Optional) Displays information only about the autonomous system boundary router summary LSAs</td>
<td>-</td>
</tr>
<tr>
<td>external</td>
<td>(Optional) Displays information only about the external LSAs</td>
<td>-</td>
</tr>
<tr>
<td>network</td>
<td>(Optional) Displays information only about the network LSAs</td>
<td>-</td>
</tr>
<tr>
<td>router</td>
<td>(Optional) Displays information only about the router LSAs</td>
<td>-</td>
</tr>
<tr>
<td>self-originate</td>
<td>(Optional) Displays only self-originated LSAs from the local router</td>
<td>-</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional) Displays information only about the summary LSAs</td>
<td>-</td>
</tr>
<tr>
<td>nssa-external</td>
<td>(Optional) Displays information only about the nssa-external LSAs</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None
Usage
None

Examples
The following is sample output from the show ip ospf database command when no arguments or keywords are used:

```
Switch# show ip ospf database

+---------------------------------+----------------+----------------+---------------+-------+--------+
<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>CkSum</th>
<th>Link count</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.1</td>
<td>10.0.0.1</td>
<td>546</td>
<td>0x80000089 0x4567</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
```

Related Commands
None

6.3.38 show ip ospf interface

Command Purpose
To display Open Shortest Path First (OSPF)-related interface information, use the show ip ospf interface command in EXEC mode.

Command Syntax

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>(Optional) Interface name. If the interface-name argument is included, only information for the specified interface is included</td>
<td>Support physical/aggregation/loopback/tunnel/vlan interfaces</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None
Examples

The following is sample output of the show ip ospf interface command when eth-0-3 is specified:

```
Switch# show ip ospf interface eth-0-3

eth-0-3 is up, line protocol is up
  Internet Address 3.3.3.1/24, Area 3 [Stub], MTU 1500
  Process ID 0, Router ID 10.0.0.1, Network Type NBMA, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.0.0.1, Interface Address 3.3.3.1
  No backup designated router on this network
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    Hello due in 00:00:17
  Neighbor Count is 1, Adjacent neighbor count is 0
  Crypt Sequence Number is 1218176990
  Hello received 0 sent 80, DD received 0 sent 0
  LS-Req received 0 sent 0, LS-Upd received 0 sent 0
  LS-Ack received 0 sent 0, Discarded 0
```

Related Commands

None

6.3.39 show ip ospf neighbor

Command Purpose

To display Open Shortest Path First (OSPF)-neighbor information on a per-interface basis, use the show ip ospf neighbor command in privileged EXEC mode.

Command Syntax

```
show ip ospf neighbor [ IFNAME ] [ NEIGHBOR-ID ] [ detail ] [ all ]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>(Optional) Interface name. If the interface-name argument is included, only information for the specified interface is included</td>
<td>-</td>
</tr>
<tr>
<td>NEIGHBOR-ID</td>
<td>(Optional) Neighbor ID</td>
<td>-</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays all neighbors given in detail (lists all neighbors)</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC
Default
None

Usage
None

Examples

The following is sample output from the show ip ospf neighbor command showing a single line of summary information for each neighbor:

Switch# show ip ospf neighbor

<table>
<thead>
<tr>
<th>Neighbor ID</th>
<th>Pri State</th>
<th>Dead Time</th>
<th>Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.199.199.137</td>
<td>1 FULL/DR</td>
<td>0:00:31</td>
<td>192.168.80.37</td>
<td>eth-0-1</td>
</tr>
<tr>
<td>172.16.48.1</td>
<td>1 FULL/DROTHER</td>
<td>0:00:33</td>
<td>172.16.48.1</td>
<td>vlan1</td>
</tr>
<tr>
<td>172.16.48.200</td>
<td>1 FULL/DROTHER</td>
<td>0:00:33</td>
<td>172.16.48.200</td>
<td>vlan2</td>
</tr>
<tr>
<td>10.199.199.137</td>
<td>5 FULL/DR</td>
<td>0:00:33</td>
<td>172.16.48.189</td>
<td>eth-0-2</td>
</tr>
</tbody>
</table>

Related Commands

None

6.3.40 show ip ospf summary-address

Command Purpose

To display the summary addresses redistribution information used by OSPF, use the show ip ospf summary-address command in privileged EXEC mode.

Command Syntax

show ip ospf summary-address

Command Mode

Privileged EXEC

Default
None
Usage

Metric equals to 16777215 means not advertise.

Examples

The following example shows how to use show ip ospf summary-address command:

Switch# show ip ospf summary-address

OSPF process 0:
10.0.0.0/8 Metric 20, Type 2, Tag 0
20.0.0.0/8 Metric 16777215, Type 0, Tag 0

Related Commands

None

6.3.41 show ip ospf database database-summary

Command Purpos

To display the summary of database used by OSPF, use the show ip ospf database database-summary command in privileged EXEC mode.

Command Syntax

show ip ospf (PROCESS-ID | ) database database-summary

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to use show ip ospf database database-summary command:

Switch# show ip ospf database database-summary

    OSPF Router with ID (10.10.10.10) (Process ID 0)
Area 0 database summary
### Related Commands

None

### 6.3.42 show ip ospf route summary

#### Command Purpose

To display the summary of routes used by OSPF, use the `show ip ospf route summary` command in privileged EXEC mode.

#### Command Syntax

```
show ip ospf (PROCESS-ID | ) route summary
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROCESS-ID</td>
<td>(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPF routing process</td>
<td>0-65535</td>
</tr>
</tbody>
</table>

#### Command Mode

Privileged EXEC

#### Default

None

#### Usage

None

#### Examples

The following example shows how to use `show ip ospf route summary` command:

```
Switch# show ip ospf route summary
```
OSPF Router with ID (10.10.10.10) (Process ID 0)

Route Type | Count
---|---
(C)Connected | 1
(D)Discard | 1
(O)Intra area | 0
(IA)Inter area | 0
(E1)Ext type 1 | 0
(E2)Ext type 2 | 0
(N1)NSSA Ext type 1 | 0
(N2)NSSA Ext type 2 | 0
Total | 2

Related Commands
None

6.3.43  show ip protocols ospf

Command Purpose
To display IP routing protocol process parameters and statistics of Open Shortest Path First (OSPF), use the show ip ospf protocols ospf command in privileged EXEC mode.

Command Syntax
show ip protocols ospf (vrf WORD )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf</td>
<td>VPN Routing/Forwarding instance</td>
<td>-</td>
</tr>
<tr>
<td>WORD</td>
<td>VPN Routing/Forwarding instance name</td>
<td>A string with 1-15 characters</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None
Examples

The following example shows how to use show ip protocols ospf command:

Switch# show ip protocols ospf

Routing Protocol is "ospf 0"
  Distributing:
  Routing for Networks:
  Distance: (default is 110)

Related Commands

None

6.3.44 show ip ospf processes-count

Command Purpose

To display the current number and max number of router ospf processes, use the show ip ospf protocols ospf command in privileged EXEC mode.

Command Syntax

show ip ospf processes-count

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to use show ip ospf process count:

DUT1# show ip ospf processes-count
Relate Commands

None

6.3.45 timers spf

Command Purpose

To set the time of Open Shortest Path First (OSPF) calculating shortest path first (SPF). To restore the default, use the no form of this command.

Command Syntax

timers spf SPF-START SPF-HOLD
no timers spf

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPF-START</td>
<td>Indicates the initial SPF schedule delay in seconds.</td>
<td>0:2147483647</td>
</tr>
<tr>
<td>SPF-HOLD</td>
<td>Indicates the minimum hold time between two consecutive SPF calculations.</td>
<td>0:2147483647</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

spf-start: 5 seconds
spf-hold: 10 seconds.

Usage

None

Examples

The following example shows a router configured with the start, and hold values for the timers spf command set at 5, and 10 seconds, respectively:

Switch# configure terminal
Switch(config)# router ospf 1
Switch(config-router)# router-id 10.10.10.2
Switch(config-router)# timers spf 5 10
Switch(config-router)# redistribute static
Switch(config-router)# network 10.21.21.0/24 area 0
Switch(config-router)# network 10.22.22.0/24 area 0

Related Commands
None

6.3.46 max-concurrent-dd

Command Purpose
To specify Maximum number allowed to process DD concurrently, use the max-concurrent-dd command in router configuration mode. To restore default value, use the no form of this command.

Command Syntax
max-concurrent-dd NUMBER-VALUE
no max-concurrent-dd

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER-VALUE</td>
<td>Number of DD process</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration

Default
5

Usage
None

Examples
The following example shows how to use max-concurrent-dd command:

Switch# configure terminal
Switch(config)# router ospf 100
Switch(config-router)# router-id 10.10.10.2
Switch(config-router)# max-concurrent-dd 10

Related Commands
None
### 6.3.47 maximum-area

#### Command Purpose

To specify Maximum number of ospf area, use the maximum-area command in router configuration mode. To restore default value, use the no form of this command

#### Command Syntax

maximum-area NUMBER-VALUE  
no maximum-area

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER-VALUE</td>
<td>Number of max-area</td>
<td>1-4294967294</td>
</tr>
</tbody>
</table>

#### Command Mode

Router Configuration

#### Default

3000

#### Usage

This command used to specify Maximum number of ospf area.

#### Examples

The following example shows how to use maximum-area command:

```
Switch# configure terminal
Switch(config)# router ospf 100
Switch(config-router)# router-id 10.10.10.2
Switch(config-router)# maximum-area 100
```

#### Related Commands

None
6.3.48 refresh timer

Command Purpose

To Set refresh timer of link state database, use the refresh timer command in router configuration mode. To restore default value, use the no form of this command.

Command Syntax

refresh timer NUMBER-VALUE
no refresh timer ( NUMBER-VALUE )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER-VALUE</td>
<td>Number of DD process</td>
<td>10-1800</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

10 seconds.

Usage

Users are not advised to modify the configuration

Examples

The following example shows how to use refresh timer command:

Switch# configure terminal
Switch(config)# router ospf 100
Switch(config-router)# router-id 10.10.10.2
Switch(config-router)# refresh timer 100

Related Commands

None

6.3.49 ip ospf bfd

Command Purpose

Use this command to enable IP BFD for ospf on an interface.
Use the “no” form of this command to disable IP BFD for ospf on an interface.

**Command Syntax**

```plaintext
ip ospf bfd
no ip ospf bfd
```

**Command Mode**

Interface Configuration

**Default**

By default IP BFD for ospf is disabled on the interface.

**Usage**

Use this command to enable IP BFD for ospf on an interface.

The IP BFD session should be created when ospf neighbor is created and the neighbor’s state is large than “two-way”.

The IP BFD session should be destroyed when ospf neighbor is delete or the neighbor’s state is not large than “two-way”.

**Examples**

In the following example, IP BFD for ospf is enabled on this interface:

```plaintext
Switch# configure terminal
Switch(config-if)# ip ospf bfd
```

**Related Commands**

None

**6.3.50 debug ospf**

**Command Purpose**

Use this command to specify all debugging options for OSPF. Use the no parameter with this command to disable this function.

**Command Syntax**

```plaintext
debug ospf (all |)
do debug ospf (all |)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>enable all debugging</td>
<td>-</td>
</tr>
</tbody>
</table>
Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
Switch# debug ospf all

Related Commands
None

6.3.51 debug ospf events

Command Purpose

Use this command to specify debugging options for OSPF event troubleshooting. Use this command without parameters to turn on all the options. Use the no parameter with this command to disable this function.

Command Syntax

ddebug ospf events {abr | asbr | lsa | os | router | vlink }

no debug ospf events {abr | asbr | lsa | os | router | vlink }

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>abr</td>
<td>Displays ABR events</td>
<td>-</td>
</tr>
<tr>
<td>asbr</td>
<td>Displays ASBR events</td>
<td>-</td>
</tr>
<tr>
<td>lsa</td>
<td>Displays LSA events</td>
<td>-</td>
</tr>
<tr>
<td>os</td>
<td>Displays OS interaction events</td>
<td>-</td>
</tr>
<tr>
<td>router</td>
<td>Displays others router events</td>
<td>-</td>
</tr>
<tr>
<td>vlink</td>
<td>Displays virtual link events</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None
Examples
Switch# debug ospf events lsa

Related Commands
None

6.3.52  debug ospf ifsm

Command Purpose
Use this command to specify debugging options for OSPF Interface Finite State Machine (IFSM) troubleshooting. Use the no parameter with this command to disable this function.

Command Syntax
debug ospf ifsm { status | events | timers }
no debug ospf ifsm { status | events | timers }

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>Displays IFSM status information</td>
<td>-</td>
</tr>
<tr>
<td>events</td>
<td>Displays IFSM event information</td>
<td>-</td>
</tr>
<tr>
<td>timers</td>
<td>Displays IFSM TIMER information</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
Switch# debug ospf ifsm timers

Related Commands
None
6.3.53 debug ospf nfsm

Command Purpose

Use this command to specify debugging options for OSPF Neighbor Finite State Machine (NFSM) troubleshooting. Use the no parameter with this command to disable this function.

Command Syntax

ddebug ospf nfsm (status | events | timers )

no debug ospf nfsm (status | events | timers )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>Displays NFSM status information</td>
<td>-</td>
</tr>
<tr>
<td>events</td>
<td>Displays NFSM event information</td>
<td>-</td>
</tr>
<tr>
<td>timers</td>
<td>Displays NFSM TIMER information</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

Switch# debug ospf nfsm timers

Related Commands

None

6.3.54 debug ospf lsa

Command Purpose

Use this command to specify debugging options for OSPF Link State Advertisements (LSA) troubleshooting. Use the no parameter with this command to disable this function.
Command Syntax

debug ospf lsa (flooding | generate | install | maxage | refresh |)

no debug ospf lsa (flooding | generate | install | maxage | refresh |)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>flooding</td>
<td>Displays LSA flooding</td>
<td>-</td>
</tr>
<tr>
<td>generate</td>
<td>Displays LSA generate</td>
<td>-</td>
</tr>
<tr>
<td>install</td>
<td>Displays LSA installation</td>
<td>-</td>
</tr>
<tr>
<td>maxage</td>
<td>Displays the maximum age of LSA in seconds</td>
<td>-</td>
</tr>
<tr>
<td>refresh</td>
<td>Displays LSA refresh</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

Switch# debug ospf lsa install

Related Commands

None

6.3.55 debug ospf packet

Command Purpose

Use this command to specify debugging options for OSPF packets.
Use the no parameter with this command to disable this function.

Command Syntax

debug ospf packet PARAMETERS
no debug ospf packet PARAMETERS

PARAMETERS = dd | detail | hello | ls-ack | ls-request | ls-update | recv | send

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dd</td>
<td>Specifies debugging for OSPF database descriptions</td>
<td>-</td>
</tr>
<tr>
<td>detail</td>
<td>Sets the debug option to detailed information</td>
<td>-</td>
</tr>
<tr>
<td>hello</td>
<td>Specifies debugging for OSPF hello packets</td>
<td>-</td>
</tr>
<tr>
<td>ls-ack</td>
<td>Specifies debugging for OSPF link state acknowledgments</td>
<td>-</td>
</tr>
<tr>
<td>ls-request</td>
<td>Specifies debugging for OSPF link state requests</td>
<td>-</td>
</tr>
<tr>
<td>ls-update</td>
<td>Specifies debugging for OSPF link state updates</td>
<td>-</td>
</tr>
<tr>
<td>recv</td>
<td>Specifies the debug option set for received packets</td>
<td>-</td>
</tr>
<tr>
<td>send</td>
<td>Specifies the debug option set for sent packets</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

Switch# debug ospf packet dd send detail

**Related Commands**

None

**6.3.56 debug ospf route**

**Command Purpose**

Use this command to specify which route calculation to debug. Use this command without parameters to turn on all the options. Use the no parameter with this command to disable this function.

**Command Syntax**

dump ospf route ( ase | ia | install | spf )

no debug ospf route ( ase | ia | install | spf )
### Command Mode

**Privileged EXEC**

### Default

None

### Usage

None

### Examples

Switch# debug ospf route install

### Related Commands

None

#### 6.3.57  show debugging ospf

**Command Purpose**

Use this command to display the set OSPF debugging option.

**Command Syntax**

`show debugging ospf`

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

This is a sample output from the `show debugging ospf` command:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ase</td>
<td>Specifies the debugging of external route calculation</td>
<td>-</td>
</tr>
<tr>
<td>ia</td>
<td>Specifies the debugging of Inter-Area route calculation</td>
<td>-</td>
</tr>
<tr>
<td>install</td>
<td>Specifies the debugging of route installation</td>
<td>-</td>
</tr>
<tr>
<td>spf</td>
<td>Specifies the debugging of SPF calculation</td>
<td>-</td>
</tr>
</tbody>
</table>
Switch# show debugging ospf

OSPF debugging status:
- OSPF packet Hello send debugging is on
- OSPF packet Database Description send debugging is on
- OSPF packet Link State Request send debugging is on
- OSPF packet Link State Update send debugging is on
- OSPF packet Link State Acknowledgment send debugging is on
- OSPF route installation debugging is on

Related Commands
None

6.3.58 show resource ospf

Command Purpose
Use this command to display the route resources used by OSPF protocol.

Command Syntax
show resource ospf

Command Mode
Privileged EXEC

Default
None

Usage
If you do not use OSPF, value of capability is 0.

Examples
The following is sample output from the show resource ospf command:

Switch# show resource ospf

OSPF
Resource    Used  Capability
===================================================
Routes      1      6144

Related Commands
show ip ospf route summary
6.4 Route Map Commands

6.4.1 route-map

Command Purpose

To define the conditions for redistributing routes from one routing protocol into another, or to enable policy routing in bgp, use the route-map command in global configuration mode and the match and set command in route-map configuration modes. To delete an entry, use the no form of this command.

Command Syntax

route-map MAP_TAG (deny | permit) (SEQUENCE-NUMBER |)
no route-map MAP_TAG (deny | permit) (SEQUENCE-NUMBER |)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAP_TAG</td>
<td>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'</td>
<td>-</td>
</tr>
<tr>
<td>permit</td>
<td>(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.</td>
<td>-</td>
</tr>
<tr>
<td>deny</td>
<td>(Optional) If the match criteria are met for the route map and the deny keyword is specified, the route is not redistributed</td>
<td>-</td>
</tr>
<tr>
<td>SEQUENCE-NUMBER</td>
<td>(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</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

The permit keyword is the default.

Usage

None
Examples

The following example shows how to create a route-map and enter route-map configuration mode:

```
Switch# configure terminal
Switch(config)# route-map rip-to-ospf permit
Switch(config-route-map)# match metric 1
Switch(config-route-map)# set metric 2
```

Related Commands

- match as-path
- match community
- match interface
- match ip address
- match local-preference
- match metric
- match origin
- match route-type
- match tag
- set aggregator
- set as-path
- set atomic-aggregate
- set comm-list
- set community
- set dampening
- set extcommunity
- set ip address
- set local-preference
- set metric
- set metric-type
- set origin
- set originator-id
- set tag
- set vpv4
- set weight

6.4.2 match as-path

Command Purpose

Use this command to match an autonomous system path access list.
Use the no parameter with this command to remove a path list entry.
The match as-path command specifies the autonomous system path to be matched. If there is a match for the specified AS path, and permit is specified, the route is redistributed or controlled, as specified by the set action. If the match criteria are met, and deny is specified, the route is not redistributed or controlled. If the match criteria are not met then the route is neither accepted nor forwarded, irrespective of permit or deny specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes, depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

**Command Syntax**

```
match as-path LISTNAME
no match as-path
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISTNAME</td>
<td>Specifies as autonomous system path access list name</td>
<td>Up to 40 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Route-map Configuration

**Default**

No match as-path is specified by default.

**Usage**

This command is valid only for BGP.

**Examples**

```
Switch# configure terminal
Switch(config)# route-map myroute deny 34
Switch(config-route-map)# match as-path myaccesslist
```

**Related Commands**

- match metric
- match ip address
- match community
- set as-path
- set community
6.4.3 match community

Command Purpose

Use this command to specify the community to be matched.
Use the no parameter with this command to remove the community list entry.
Communities are used to group and filter routes. They are designed to provide the ability to apply policies to large numbers of routes by using match and set commands. Community lists are used to identify and filter routes by their common attributes.
Use the match community command to allow matching based on community lists.
The values set by the match community command overrides the global values. The route that does not match at least one match clause is ignored.

Command Syntax

match community WORD
no match community

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>Specifies the Community-list name</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode

Route-map Configuration

Default

No match community is specified by default.

Usage

This command is valid only for BGP.

Examples

Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# match community mylist

Related Commands

match ip address
match as-path
set as-path
set community
match metric
6.4.4  match interface

Command Purpose

Use this command to define the interface match criterion.
Use the no parameter with this command to remove the specified match criterion.
The match interface command specifies the next-hop interface name of a route to be matched.

Command Syntax

match interface IFNAME
no match interface

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>A string that specifies the interface for matching</td>
<td>Support physical/aggregation/loopback/tunnel/vlan interfaces</td>
</tr>
</tbody>
</table>

Command Mode

Route-map Configuration

Default

No match interface is specified by default.

Usage

This command is valid only for OSPF.

Examples

Switch# configure terminal
Switch(config)# route-map mymap1 permit 10
Switch(config-route-map)# match interface eth-0-1

Related Commands

match tag
match route-type external

6.4.5  match ip address

Command Purpose

Use this command to specify the match address of route.
Use the no parameter with this command to remove the match ip address entry.
The match ip address command specifies the IP address to be matched. If there is a match for the specified IP address, and permit is specified, the route is redistributed or controlled, as specified by the set action. If the match criteria are met, and deny is specified then the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of permit or deny specifications.
The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes, depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

**Command Syntax**

```plaintext
match ip address ACCESSLISTID
no match ip address
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCESSLISTID</td>
<td>Specify an IPv4 access-list name, up to 20 characters</td>
<td></td>
</tr>
</tbody>
</table>

**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**

```plaintext
Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# match ip address List1
```

**Related Commands**

match community
match as-path
set as-path
set community
match metric

6.4.6 match ip address prefix-list

**Command Purpose**

Use this command to match entries of prefix-lists. Use the no parameter with this command to disable this function.
This command specifies the entries of prefix-lists to be matched. If there is a match for the specified prefix-list entries, and permit is specified, the route is redistributed or controlled, as specified by the set action. If the match criteria are met, and deny is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of permit or deny specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

**Command Syntax**

```plaintext
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**

```plaintext
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# match ip address prefix-list mylist
```

**Related Commands**

match community
match as-path
set as-path
set community
match metric

6.4.7 match ip next-hop

**Command Purpose**

Use this command to specify a next-hop address to be matched in a route-map.

Use the no parameter with this command to disable this function.

The match ip next-hop command specifies the next-hop address to be matched. If there is a match for the specified next-hop address, and permit is specified, the route is redistributed or controlled as specified by the set action. If the match criteria are met, and deny is specified,
the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of permit or deny specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

**Command Syntax**

```
match ip next-hop ACCESSSLISTID
no match ip next-hop [ACCESSSLISTID]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCESSSLISTID</td>
<td>Specify an IPv4 access-list name, up to 20 characters</td>
<td>Up to 40 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Route-map Configuration

**Default**

No match ip next-hop is specified by default.

**Usage**

This command is valid for BGP, OSPF and RIP only.

**Examples**

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# match ip next-hop mylist
```

**Related Commands**

match community
match as-path
set as-path
set community
match metric

6.4.8 match ip next-hop prefix-list

**Command Purpose**

Use this command to specify the next-hop IP address match criterion, using the prefix-list.

Use the no parameter with this command to remove the specified match criterion.
**Command Syntax**

match ip next-hop prefix-list LISTNAME
no match ip next-hop prefix-list [ LISTNAME ]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISTNAME</td>
<td>A string specifying the prefix-list name</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Route-map Configuration

**Default**

No match ip next-hop prefix-list is specified by default.

**Usage**

This command is valid for BGP, OSPF and RIP only.

**Examples**

Switch# configure terminal
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# match ip next-hop prefix-list list1

**Related Commands**

match metric
match interface
match ip next-hop

**6.4.9 match local-preference**

**Command Purpose**

Use this command to specify the local-preference match criterion.
Use the no parameter with this command to remove the specified match criterion.
Use the match local-preference command to match the local preference of a route.

**Command Syntax**

match local-preference LOCAL-PREFERENCE
no match local-preference

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOCAL-PREFERENCE</td>
<td>Species the preference value</td>
<td>0-4294967295</td>
</tr>
</tbody>
</table>
**Command Mode**

Route-map Configuration

**Default**

No match local-preference is specified by default.

**Usage**

This command is valid for BGP only.

**Examples**

```
Switch# configure terminal
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# match local-preference 100
```

**Related Commands**

match community
match as-path
set as-path
set community
match ip next-hop

### 6.4.10 match metric

**Command Purpose**

Use this command to match a metric of a route.

Use the no parameter with this command to disable this function.

The match metric command specifies the metric to be matched. If there is a match for the specified metric, and permit is specified, the route is redistributed or controlled as specified by the set action. If the match criteria are met, and deny is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of permit or deny specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

**Command Syntax**

```
match metric METRICVAL
```
no match metric

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>METRICVAL</td>
<td>The metric value</td>
<td>0-4294967295</td>
</tr>
</tbody>
</table>

**Command Mode**

Route-map Configuration

**Default**

No match metric is specified by default.

**Usage**

This command is valid for BGP, OSPF and RIP only.

**Examples**

Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# match metric 2

**Related Commands**

match community
match as-path
set as-path
set community
match ip next-hop

**6.4.11 match origin**

**Command Purpose**

Use this command to match origin code.
Use the no parameter with this command to disable this matching.
The origin attribute defines the origin of the path information. The egp parameter is indicated as an e in the routing table, and it indicates that the origin of the information is learned via Exterior Gateway Protocol. The igr 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>egp</td>
<td>learned from EGP</td>
<td>-</td>
</tr>
<tr>
<td>igp</td>
<td>Local IGP</td>
<td>-</td>
</tr>
<tr>
<td>incomplete</td>
<td>Unknown heritage</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Route-map Configuration

**Default**

No match origin is specified by default.

**Usage**

This command is valid for BGP only.

**Examples**

Switch# configure terminal
Switch(config)# route-map myroute deny 34
Switch(config-route-map)# match origin egp

**Related Commands**

None

6.4.12 match route-type external

**Command Purpose**

Use this command to match specified external route type.
Use the no parameter with this command to turn off the matching.
Use the match route-type external command to match specific external route types. AS-external LSA is either Type-1 or Type-2. External type-1 matches only Type 1 external routes, and external type-2 matches only Type 2 external routes.

**Command Syntax**

```
match route-type external { type-1 | type-2 }
no match route-type external
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>type-1</td>
<td>Match OSPF External Type 1 metrics</td>
<td>-</td>
</tr>
<tr>
<td>type-2</td>
<td>Match OSPF External Type 1 metrics</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Route-map Configuration

**Default**

No match route-type is specified by default.

**Usage**

This command is valid for OSPF only.

**Examples**

```
Switch# configure terminal
Switch(config)# route-map mymap1 permit 10
Switch(config-route-map)# match route-type external type-1
```

**Related Commands**

match tag

**6.4.13  match tag**

**Command Purpose**

Use this command to match the specified tag value.

Use the no parameter with this command to turn off the declaration.

Use the match tag command to match the specified tag value.
Command Syntax

match tag TAG
no match tag

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TAG</td>
<td>Specifies the tag value</td>
<td>0-4294967295</td>
</tr>
</tbody>
</table>

Command Mode

Route-map Configuration

Default

No match tag is specified by default.

Usage

This command is valid for OSPF RIP only.

Examples

Switch# configure terminal
Switch(config)# route-map mymap1 permit 10
Switch(config-route-map)# match tag 100

Related Commands

match metric
match route-type external

6.4.14 set aggregator

Command Purpose

Use this command to set the AS number for the route map and router ID.

Use the no parameter with this command to disable this function.

An Autonomous System (AS) is a collection of networks under a common administration sharing a common routing strategy. It is subdivided by areas, and is assigned a unique 16-bit number. Use the set aggregator command to assign an AS number for the aggregator.

To use the set aggregator command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.
Command Syntax

set aggregator as ASNUM IPADDRESS
no set aggregator

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASNUM</td>
<td>Specifies the AS number of aggregator</td>
<td>1-65535</td>
</tr>
<tr>
<td>IPADDRESS</td>
<td>Specifies the IP address of aggregator</td>
<td>-</td>
</tr>
</tbody>
</table>

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 43.10.0.3

Related Commands

None

6.4.15 set as-path

Command Purpose

Use this command to modify an autonomous system path for a route.
Use the no parameter with this command to disable this function.
Use the set as-path command to specify an autonomous system path. By specifying the length of the AS-Path, the router influences the best path selection by a neighbor. this command to prepend an AS path string to routes increasing the AS path length.
To use the set as-path command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.
If the packets do not match any of the defined criteria, they are routed through the normal routing process.
**Command Syntax**

```
set as-path prepend ASN [ ...ASN ]
no set as-path
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASN</td>
<td>System prepends this number to the AS path or overwrite the AS path</td>
<td>1-4294967295</td>
</tr>
</tbody>
</table>

**Command Mode**

Route-map Configuration

**Default**

No set as-path is specified by default.

**Usage**

This command is valid for BGP only.

**Examples**

```
Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# set as-path prepend 8 24
```

**Related Commands**

None

**6.4.16 set atomic-aggregate**

**Command Purpose**

Use this command to set an atomic aggregate attribute.

Use the no parameter with this command to disable this function.

To use the set atomic aggregate command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met. If the packets do not match any of the defined criteria, they are routed through the normal routing process.

**Command Syntax**

```
set atomic-aggregate
no set atomic-aggregate
```
Command Mode

Route-map Configuration

Default

No set atomic-aggregate is specified by default.

Usage

This command is valid for BGP only.

Examples

Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set atomic-aggregate

Related Commands

None

6.4.17 set comm-list delete

Command Purpose

Use this command to delete the matched communities from the community attribute of an inbound or outbound update when applying route-map.

Use the no parameter with this command to disable this feature.

Command Syntax

set comm-list {STANDARD_ID | EXPANDED_ID | WORD} delete
no set comm-list

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>STANDARD_ID</td>
<td>Standard community-list number</td>
<td>1-99</td>
</tr>
<tr>
<td>EXPANDED_ID</td>
<td>Expanded community-list number</td>
<td>100-199</td>
</tr>
<tr>
<td>WORD</td>
<td>Name of the Community-list</td>
<td>A string with 1-20 characters, the first character should be among [a-zA-Z0-9]</td>
</tr>
<tr>
<td>delete</td>
<td>Delete matching communities</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Route-map Configuration
Default
No set comm-list is specified by default.

Usage
This command is valid for BGP only.

Examples
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set comm-list 34 delete

Related Commands
None

6.4.18 set community

Command Purpose
Use this command to set the communities attribute.
Use the no parameter with this command to delete the entry.
Use this command to set the community attribute and group destinations in a certain community, as well as, apply routing decisions according to those communities.
To use the set community command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.
If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax
set community { AA:NN | internet | local-AS | no-advertise | no-export }
set community none
no set community

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA:NN</td>
<td>AA:NN: Specifies the community number in this format</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AA = The AS number</td>
<td>AA is in the range 1-65535</td>
</tr>
<tr>
<td></td>
<td>NN = The number assigned to community</td>
<td></td>
</tr>
<tr>
<td>internet</td>
<td>Specifies the Internet (well-known community)</td>
<td>-</td>
</tr>
<tr>
<td>local-AS</td>
<td>Specifies no sending outside the local AS (well-known community)</td>
<td>-</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Specifies no advertisement of this route to any peer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(well-known community)</td>
<td>-</td>
</tr>
<tr>
<td>no-export</td>
<td>Specifies no advertisement of this route to next AS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(well-known community)</td>
<td>-</td>
</tr>
<tr>
<td>none</td>
<td>Removes the community attribute from the prefixes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>that pass the route-map</td>
<td>-</td>
</tr>
</tbody>
</table>
**Command Mode**

Route-map Configuration

**Default**

No set community is specified by default.

**Usage**

This command is valid for BGP only.

**Examples**

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set community no-export no-advertise
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set community no-advertise
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set community 10:01 23:34 12:14 no-export
```

**Related Commands**

None

**6.4.19 set dampening**

**Command Purpose**

Use this command to enable route-flap dampening and set parameters. Use the no parameter with this command to disable it. Set the unreachability half-life time to be equal to, or greater than, reachability half-life time. The suppress-limit value must be greater than or equal to the reuse limit value.

**Command Syntax**

```
set dampening REACHTIME REUSE SUPPRESS MAXSUPPRESS [ UNREACHTIME ]
no set dampening
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>REACHTIME</td>
<td>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.</td>
<td>1-45</td>
</tr>
<tr>
<td>REUSE</td>
<td>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.</td>
<td>1-20000</td>
</tr>
<tr>
<td>SUPPRESS</td>
<td>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.</td>
<td>1-20000</td>
</tr>
<tr>
<td>MAXSUPPRESS</td>
<td>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).</td>
<td>1-255</td>
</tr>
<tr>
<td>UNREACHTIME</td>
<td>Specifies the un-reachability half-life time for penalty, in minutes. The default value is 15 minutes.</td>
<td>1-45</td>
</tr>
</tbody>
</table>

Command Mode

Route-map Configuration

Default

Reference to the syntax description above.

Usage

This command is valid for BGP only.

Examples

Switch# configure terminal
Switch(config)# route-map R1 permit 24
Switch(config-route-map)# set dampening 20 333 534 30

Related Commands

None

6.4.20 set extcommunity

Command Purpose

Use this command to set an extended community attribute.

Use the no parameter with this command to disable this function

To use the set extcommunity command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.
Command Syntax

set extcommunity { rt | soo } EXTCOMMNUMBER [ …EXTCOMMNUMBER ]
no set extcommunity { rt | soo }

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>rt</td>
<td>Specifies the route target of the extended community</td>
<td>-</td>
</tr>
<tr>
<td>soo</td>
<td>Specifies the site-of-origin of the extended community</td>
<td>-</td>
</tr>
<tr>
<td>EXTCOMMNUMBER</td>
<td>ASN:NN or IP-address</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>nn VPN extended community</td>
<td>-</td>
</tr>
<tr>
<td>ASN:NN</td>
<td>the AS number</td>
<td>ASN is in the range 1-65535</td>
</tr>
<tr>
<td></td>
<td>NN is in the range of 1-65535</td>
<td></td>
</tr>
<tr>
<td>IPADDRESS</td>
<td>the AS number in IP address form</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
</tbody>
</table>

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 rmap1 permit 3
Switch(config-route-map)# set extcommunity soo 0.0.0.6:01

Related Commands

None
6.4.21 set ip next-hop

**Command Purpose**

Use this command to set the specified next-hop value.
Use the no parameter with this command to turn off the setting.
Use this command to set the next-hop IP address to the routes.

**Command Syntax**

```
set ip next-hop A.B.C.D (track object_id |)
no set ip next-hop (track |)
```

**Parameter** | **Parameter Description** | **Parameter Value**
--- | --- | ---
A.B.C.D | Specifies the IP address of the next-hop | IPv4 Address in A.B.C.D format
object_id | Object identity is used to identify track object | 1-500

**Command Mode**

Route-map Configuration

**Default**

No set ip next-hop is specified by default.

**Usage**

This command is valid for BGP, OSPF, RIP and PBR only. Configuring the set ip next-hop command causes the system to use policy-based routing first and then use the routing table. Configured with track command will bind nexthop with track, when track down, the nexthop will be invalided. Use the no command with track will unbind nexthop with track.

**Examples**

The following example shows how to set the next-hop IP address:

```
Switch# configure terminal
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# set ip next-hop 10.10.0.67
```

The following example shows how to set the next-hop IP address and bind with track:

```
Switch# configure terminal
Switch(config)# track 1 interface eth-0-1 linkstate
Switch(config-track)# quit
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# set ip next-hop 10.10.0.67 track 1
```

**Related Commands**

None
6.4.22 set 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOCAL-PREFERENCE</td>
<td>Species the preference value</td>
<td>0-4294967295</td>
</tr>
</tbody>
</table>

Command Mode

Route-map Configuration

Default

No set local-preference is specified by default.

Usage

This command is valid for BGP only.

Examples

Switch# configure terminal
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# set local-preference 100

Related Commands

None

6.4.23 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**

```bash
set metric METRICVAL
no set metric
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>METRICVAL</td>
<td>The metric value</td>
<td>0-4294967295</td>
</tr>
</tbody>
</table>

**Command Mode**

Route-map Configuration

**Default**

No set metric is specified by default.

**Usage**

This command is valid for BGP, OSPF and RIP.

**Examples**

```bash
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set metric 600
```

**Related Commands**

None

**6.4.24 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>type1</td>
<td>Select to set external type 1 metric</td>
<td>-</td>
</tr>
<tr>
<td>type2</td>
<td>Select to set external type 2 metric</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Route-map Configuration

Default

No set metric-type is specified by default.

Usage

This command is valid for OSPF only.

Examples

Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set metric-type 1

Related Commands

None

6.4.25 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
### Command Mode

**Route-map Configuration**

**Default**

No set origin is specified by default.

**Usage**

This command is valid for BGP only.

**Examples**

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set origin egp
```

**Related Commands**

None

#### 6.4.26 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPADDRESS</td>
<td>Specifies the IP address of originator</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
</tbody>
</table>
Command Mode

Route-map Configuration

Default

No set originator-id is specified by default.

Usage

This command is valid for BGP only.

Examples

Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set originator-id 1.1.1.1

Related Commands

None

6.4.27 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TAGVALUE</td>
<td>Tag value for destination routing protocol.</td>
<td>0-4294967295</td>
</tr>
</tbody>
</table>

Command Mode

Route-map Configuration
Default

No set tag is specified by default.

Usage

This command is valid for OSPF and RIP only.

Examples

Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set tag 6

Related Commands

redistribute
default-information

6.4.28 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPADDRESS</td>
<td>Specifies the IP address of next-hop</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
</tbody>
</table>

Command Mode

Route-map Configuration

Default

No set vpnv4 next-hop is specified by default.

Usage

This command is valid for BGP only.
Examples

Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set vpnv4 next-hop 6.6.6.6

Related Commands

None

6.4.29 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEIGHT</td>
<td>Specifies the weight value</td>
<td>0-4294967295</td>
</tr>
</tbody>
</table>

Command Mode

Route-map Configuration

Default

No set weight is specified by default.

Usage

This command is valid for BGP only.

Examples

Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set weight 60

Related Commands

match as-path
6.4.30 show route-map

Command Purpose
Use this command to display user readable route-map information.

Command Syntax
show route-map (NAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>route-map name</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
Switch1# show route-map
route-map abc, permit, sequence 10
  Match clauses:
  ip address acl1
  Set clauses:
    local-preference 200
route-map abc, permit, sequence 20
  Match clauses:
  Set clauses:

Related Commands
route-map

6.5 Prefix-list Commands

6.5.1 ip prefix-list

Command Purpose
To create a prefix list or add a prefix-list entry, use the ip prefix-list command in global configuration mode. To delete a prefix-list or an entry, use the no form of this command.
Command Syntax

```
ip prefix-list WORD ( seq SEQUENCE-NUMBER | ( deny | permit ) ( any | A.B.C.D/M ( ge GE-LENGTH | ( le LE-LENGTH ) ) | ( any | A.B.C.D/M ( ge GE-LENGTH | ( le LE-LENGTH ) ) )
no ip prefix-list WORD ( seq SEQUENCE-NUMBER | ( deny | permit ) ( any | A.B.C.D/M ( ge GE-LENGTH | ( le LE-LENGTH ) )
no ip prefix-list WORD ( seq SEQUENCE-NUMBER )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>Config a name to identify the prefix list</td>
<td>Up to 40 characters</td>
</tr>
<tr>
<td>seq SEQUENCE-NUMBER</td>
<td>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</td>
<td>1-65535</td>
</tr>
<tr>
<td>deny</td>
<td>Denies access for a matching condition</td>
<td>-</td>
</tr>
<tr>
<td>permit</td>
<td>Permits access for a matching condition</td>
<td>-</td>
</tr>
<tr>
<td>A.B.C.D/M</td>
<td>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</td>
<td>IPv4 Address and mask length in A.B.C.D/M format</td>
</tr>
<tr>
<td>ge GE-LENGTH</td>
<td>(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</td>
<td>1-32</td>
</tr>
<tr>
<td>le LE-LENGTH</td>
<td>(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</td>
<td>1-32</td>
</tr>
</tbody>
</table>

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
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 incremented by 5 (for example, 5, 10, 15, and onwards). If a sequence number is entered for the first prefix list entry but not subsequent entries, then the subsequent entries will also be incremented by 5 (for example, if the first configured sequence number is 3, then subsequent entries will be 8, 13, 18, and onwards). Default sequence numbers can be suppressed by entering the no form of this command with the seq keyword. Prefix lists are evaluated starting with the lowest sequence number and continues down the list until a match is made. Once a match is made that covers the network the permit or deny statement is applied to that network and the rest of the list is not evaluated.

**Examples**

To deny the default route 0.0.0.0/0:
```
Switch# configure terminal
Switch(config)# ip prefix-list abc deny 0.0.0.0/0
```

To permit the prefix 10.0.0.0/8:
```
Switch# configure terminal
Switch(config)# ip prefix-list abc permit 10.0.0.0/8
```

To accept a mask length of up to 24 bits in routes with the prefix 192/16:
```
Switch# configure terminal
Switch(config)# ip prefix-list abc permit 192.168.0.0/16 le 24
```

To deny mask lengths greater than 25 bits in routes with the prefix 192/16:
```
Switch# configure terminal
Switch(config)# ip prefix-list abc deny 192.168.0.0/16 ge 25
```

**Related Commands**

- `ip prefix-list description`
- `ip prefix-list sequence`
- `show ip prefix-list`
- `clear ip prefix-list`

### 6.5.2 `ip prefix-list description`

**Command Purpose**

To add a text description of a prefix list, use the `ip prefix-list description` command in global configuration mode. To remove the text description, use the `no` form of this command.

**Command Syntax**

```
ip prefix-list WORD description LINE
```
no ip prefix-list WORD description (LINE)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>Name of prefix list</td>
<td>Up to 40 characters</td>
</tr>
<tr>
<td>LINE</td>
<td>Up to 80 characters describing this prefix-list</td>
<td>Up to 80 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

There is no description for prefix-list.

**Usage**

The prefix list will be created automatically if it didn’t exist.

**Examples**

The following example shows how to add description:

Switch# configure terminal
Switch(config)# ip prefix-list abc description Deny routes from router A

**Related Commands**

ip prefix-list
ip prefix-list sequence
show ip prefix-list
clear ip prefix-list

6.5.3 ip prefix-list sequence-number

**Command Purpose**

To enable the generation of sequence numbers for entries in a prefix list, use the `ip prefix-list sequence-number` command in global configuration mode. To disable this function, use the `no` form of this command.

**Command Syntax**

ip prefix-list sequence-number
no ip prefix-list sequence-numbe

**Command Mode**

Global Configuration
Default
This command has no default behavior.

Usage
This command is used to enable sequence-number display.

Examples
The following example shows how to enable ip prefix-list sequence-number:

Switch# configure terminal
Switch(config)# ip prefix-list sequence-number

Related Commands
ip prefix-list
show ip prefix-list
clear ip prefix-list

6.5.4 show ip prefix-list

Command Purpose
To show prefix list information, use the show ip prefix-list command.

Command Syntax

show ip prefix-list ( summary | detail | ) ( WORD )
show ip prefix-list WORD ( seq SEQUENCE-NUMBER | A.B.C.D/M ( longer | first-match | ) )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>Summary of prefix lists</td>
<td>-</td>
</tr>
<tr>
<td>detail</td>
<td>Detail of prefix lists</td>
<td>-</td>
</tr>
<tr>
<td>WORD</td>
<td>Name of the prefix list</td>
<td>Up to 40 characters</td>
</tr>
<tr>
<td>seq SEQUENCE-NUMBER</td>
<td>sequence number of the entry in the prefix list</td>
<td>1-65535</td>
</tr>
<tr>
<td>A.B.C.D/M</td>
<td>IPv4 prefix &lt;network&gt;/&lt;length&gt;, e.g., 35.0.0.0/8</td>
<td>IPv4 Address and mask length in A.B.C.D/M format</td>
</tr>
<tr>
<td>longer</td>
<td>Lookup the mask of prefix longer than M</td>
<td>-</td>
</tr>
<tr>
<td>first-match</td>
<td>First matched prefix</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC
Default

This command has no default behavior.

Usage

None

Examples

The following example shows how to display ip prefix-list:

```
Switch# show ip prefix-list
ip prefix-list aa: 2 entries
    permit 1.1.1.0/24
    permit 1.2.3.0/24
```

Related Commands

ip prefix-list
clear ip prefix-list

6.5.5 clear ip prefix-list

Command Purpose

To resets the hit count of the prefix list entries, use the clear ip prefix-list command.

Command Syntax

```
clear ip prefix-list (WORD (A.B.C.D/M | ) )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>Name of the prefix list</td>
<td>Up to 40 characters</td>
</tr>
<tr>
<td>A.B.C.D/M</td>
<td>IP prefix &lt;network&gt;/&lt;length&gt;, e.g., 35.0.0.0/8</td>
<td>IPv4 Address and mask length in A.B.C.D/M format</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None
Usage

None

Examples

The following example shows how to clear ip prefix-list:

Switch# clear ip prefix-list abc

Related Commands

ip prefix-list

6.6 Policy-Based Routing Commands

6.6.1 ip policy route-map

Command Purpose

By default, PBR is disabled on the switch. To enable PBR, you must create a route map that specifies the match criteria and the resulting action if all of the match clauses are met. Then, you must enable PBR on a layer3 interface. All packets arriving on the specified interface matching the match clauses are subject to PBR.

Command Syntax

ip policy route-map MAP_NAME
no ip policy route-map

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAP_NAME</td>
<td>policy route-map name</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

Disabled

Usage

This command can only be configured on routed port, vlan interface and routed agg port.
Examples

The following example shows how to configure pbr on an interface:

```
Switch# configure terminal
switch (config)# ip access-list 1 extend
switch (config-ex-ip-accl)# 10 permit any any
switch (config-route-map)#exit
switch (config)#route-map richard permit 10
switch (config-route-map)#match ip address 1
switch (config-route-map)#set ip next-hop 10.1.1.1
switch (config-route-map)#exit
switch (config)#interface eth-0-1
switch (config-if)#no switch port
switch (config-if)#no shutdown
switch (config-if)#ip policy route-map richrad
```

Related Commands

route-map

6.6.2 show ip policy route-map

Command Purpose

Use this command to display user readable policy route-map information

Command Syntax

```
show ip policy route-map
```

Command Mode

Privileged EXEC

Default

Disabled

Usage

If some of the PBR entries are not successfully inserted into tcam, an error tip will be displayed.
Examples

SWITCH# show ip policy route-map

Route-map                  interface
richard                   eth-0-1
                          eth-0-3
Failed entry: no
sally                     eth-0-2
Failed entry: yes

Please use Policy Based-Routing CLI: show pbr failed entry to gain more detail.

Related Commands

route-map

6.6.3 show resource pbr

Command Purpose

Use this command to display the resource usage over the policy based routing module.

Command Syntax

show resource pbr

Command Mode

Privileged EXEC

Default

Disabled

Usage

None

Examples

SWITCH# show resource pbr

<table>
<thead>
<tr>
<th>Policy Based Routing</th>
<th>Resource</th>
<th>Used</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Parameter Description</td>
<td>Parameter Value</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------</td>
<td>-----------------</td>
<td></td>
</tr>
<tr>
<td>vpnv4</td>
<td>Configures sessions for VPN-IPv4 prefixes. This parameter takes an IPv4 style address: A.B.C.D.</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>unicast</td>
<td>Specifies unicast prefixes</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>vrf</td>
<td>VPN routing/forwarding instance</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>NAME</td>
<td>VPN Routing/Forwarding instance name</td>
<td>Up to 15 characters</td>
<td></td>
</tr>
</tbody>
</table>

**Related Commands**

route-map  
show ip policy route-map

## 6.7 BGP Commands

### 6.7.1 address-family

**Command Purpose**

Use this command to enter the IPv4, VPNv4 address-family command mode.

**Command Syntax**

address-family ipv4 ( unicast | vrf NAME )
adress-family vpnv4 ( unicast )

**Command Mode**

Router Configuration

**Default**

None

**Usage**

Use the address family command to enter the address family mode allowing configuration of address-family specific parameters. To leave the address family mode and return to the Configure mode use the exit-address-family command.

**Examples**

Switch# configure terminal  
Switch(config) router bgp 100  
Switch(config-router)address-family ipv4
Related Commands

exit-address-family
Exit

6.7.2 aggregate-address

Command Purpose

Use this command to configure BGP aggregate entries.
Use the no parameter with this command to disable this function.

Command Syntax

( no ) aggregate-address IP_PREFIX { summary-only | as-set }

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_PREFIX</td>
<td>A.B.C.D/M Specifies the aggregate prefix</td>
<td>IPv4 Address and mask length in A.B.C.D/M format</td>
</tr>
<tr>
<td>summary-only</td>
<td>Filters more specific routes from updates.</td>
<td></td>
</tr>
<tr>
<td>as-set</td>
<td>Generates AS set path information</td>
<td></td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

Disabled

Usage

Aggregates are used to minimize the size of routing tables. Aggregation combines the characteristics of several different routes and advertises a single route. The aggregate-address command creates an aggregate entry in the BGP routing table if any more-specific BGP routes are available in the specified range. Using the summary-only parameter advertises the prefix only, suppressing the more-specific routes to all neighbors.

Examples

Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# aggregate-address 10.0.0.0/8 as-set summary-only
Related Commands

N/A

6.7.3 bgp always-compare-med

Command Purpose

Use this command to compare the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems. Use the no parameter with this command to disallow the comparison.

Command Syntax

(no) bgp always-compare-med

Command Mode

Router Configuration

Default

Disabled

Usage

Multi Exit Discriminator (MED) is used in best path selection by BGP. MED is compared after BGP attributes weight, local preference, AS-path and origin have been compared and are equal. MED comparison is done only among paths from the same autonomous system (AS). Use bgp always-comparemed command to allow comparison of MEDs from different ASs. The MED parameter is used to select the best path. A path with lower MED is preferred.

Examples

Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp always-compare-med

Related Commands

bgp bestpath med
bgp bestpath as-path ignore

6.7.4 bgp bestpath as-path ignore
Command Purpose

Use this command to prevent the router from considering as-path as a factor in the algorithm for choosing a route.
Use the no parameter with this command to allow the router to consider as-path in choosing a route.

Command Syntax

( no ) bgp bestpath as-path ignore

Command Mode

Router Configuration

Default

Disabled

Usage

None

Examples

Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp bestpath as-path ignore

Related Commands

bgp always-compare-med, bgp bestpath med, bgp bestpath compare-routerid

6.7.5 bgp bestpath compare-confed-aspath

Command Purpose

Use this command to allow comparing of the confederation AS path length.
Use the no parameter with this command to revert the selection and ignore AS confederation path length in the BGP best path selection.

Command Syntax

( no ) bgp bestpath compare-confed-aspath
Command Mode
Router Configuration

Default
BGP receives routes with identical eBGP paths from eBGP peers and selects the first route received as the best path.

Usage
This command specifies that the AS confederation path length must be used, when available, in the BGP best path decision process. It is effective only when bgp bestpath as-path ignore command has not been specified.

Examples
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp bestpath compare-confed-aspath

Related Commands
bgp bestpath as-path ignore

6.7.6 bgp bestpath compare-routerid

Command Purpose
Use this command to compare router-id for identical eBGP paths.
Use the no parameter with this command to disable this function.

Command Syntax
( no ) bgp bestpath compare-routerid

Command Mode
Router Configuration

Default
BGP receives routes with identical eBGP paths from eBGP peers and selects the first route received as the best path.

Usage
When comparing similar routes from peers the BGP router does not consider router ID of the routes. By default, it selects the first received route. Use this command to include router ID in the selection process; similar routes are compared and the route with lowest router ID is selected. The router-id is the highest IP address on the router, with preference given to loopback addresses. Router-id can be manually set by using the bgp router-id command.

Examples
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp bestpath compare-routerid
Related Commands
show ip bgp
show ip bgp neighbors

6.7.7 bgp bestpath med

Command Purpose
Use this command to specify Multi Exit Discriminator (MED) attribute comparison.
Use the no parameter with this command to prevent BGP from considering the MED attribute in comparing paths.

Command Syntax
bgp bestpath med confed [ missing-as-worst ]
bgp bestpath med missing-as-worst [ confed ]
no bgp bestpath med confed [ missing-as-worst ]
no bgp bestpath med missing-as-worst [ confed ]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>confed</td>
<td>Compares MED among confederation paths</td>
<td>-</td>
</tr>
<tr>
<td>missing-as-worst</td>
<td>Treats missing MED as the least preferred one</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration

Default
MED value is zero.

Usage
Use this command to specify two MED attributes – confed and missing-as-worst. The confed attribute enables MED comparison among paths learned from confederation peers. The MEDs are compared only if there is no external autonomous system (an AS not within the confederation) in the path. If there is an external autonomous system in the path, the MED comparison is not made.
The missing-as-worst attribute to consider a missing MED attribute in a path as having a value of infinity, making the path without a MED value the least desirable path. If missing-as-worst is disabled, the missing MED is assigned the value of 0, making the path with the missing MED attribute the best path.

Examples
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp bestpath med missing-as-worst

Related Commands
bgp-always-compare-med, bgp bestpath as-path ignore, bgp deterministic-med
6.7.8 bgp client-to-client reflection

Command Purpose

Use this command to restore route reflection from a BGP route reflector to clients.
Use the no parameter with this command to turn off client-to-client reflection.

Command Syntax

bgp client-to-client reflection
no bgp client-to-client reflection

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>reflection</td>
<td>Allows reflection of routes</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

When a router is configured as a route reflector, client-to-client reflection is enabled by default.

Usage

The bgp client-to-client reflection command is used to configure routers as route reflectors. Route reflectors are used when all Interior Border Gateway Protocol (iBGP) speakers are not fully meshed. If the clients are fully meshed the route reflector is not required, use no bgp client-to-client reflection command to disable the client-to-client route reflection.

Examples

Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) no bgp client-to-client reflection

Related Commands

bgp cluster-id
neighbor route-reflector-client
show ip bgp
6.7.9 bgp cluster-id

Command Purpose

Use this command to configure the cluster ID if the BGP cluster has more than one route reflector. Use the no parameter with this command to remove the cluster ID.

Command Syntax

bgp cluster-id CLUSTERID
no bgp cluster-id

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLUSTERID</td>
<td>Specifies the cluster ID of this router acting as a route reflector, either as IP address or as a maximum of 4 bytes.</td>
<td>IPv4 Address in A.B.C.D format or number in range 1-4294967295</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>A.B.C.D Route Reflector Cluster-id in IP address format</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>1-4294967295</td>
<td>Route Reflector cluster-id as a 32 bit quantity</td>
<td>1-4294967295</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

N/A

Usage

A cluster includes route reflectors and its clients. Usually, each cluster is identified by the router ID of its single route reflector but to increase redundancy sometimes a cluster may have more than one route reflector. All router reflectors in such a cluster are then identified by a cluster ID. The bgp cluster-id command is used to configure the 4 byte cluster ID for clusters with more than one route reflectors.

Examples

Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp cluster-id 1.1.1.1

Related Commands

bgp client-to-client reflection, neighbor route-reflector-client, show ip bgp
6.7.10 bgp confederation identifier

Command Purpose

Use this command to specify a Bgp confederation identifier.
Use the no parameter with this command to remove the Bgp confederation identifier.

Command Syntax

bgp confederation identifier ID
no bgp confederation identifier

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Set routing domain confederation AS number</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

N/A

Usage

N/A

Examples

Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp confederation identifier 1

Related Commands

bgp confederation peer

6.7.11 bgp confederation peers

Command Purpose

Use this command to configure the Autonomous Systems (AS) that belong to the confederation.
Use the no parameter with this command to remove an autonomous system from the confederation.
Command Syntax

bgp confederation peers .ASN
no bgp confederation peers (.ASN |)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASN</td>
<td>AS numbers of eBGP peers that are under same confederation but in a different sub-AS</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

N/A

Usage

A confederation allows an AS to be divided into several ASs. The AS is given a confederation identifier. External routers view only the whole confederation as one AS. Each AS is fully meshed within itself and is visible internally to the confederation. Use the bgp confederation peer command to define the list of confederation peers.

Examples

Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp confederation peers 1234 21345

Related Commands

bgp confederation identifier

6.7.12 bgp dampening

Command Purpose

Use this command to set bgp dampening parameters.
Use the no parameter with this command to unset the bgp dampening parameters.

Command Syntax

bgp dampening REACHTIME
bgp dampening REACHTIME REUSE
bgp dampening REACHTIME REUSE SUPPRESS MAXSUPPRESS ( UNREACHTIME | )
bgp dampening route-map ROUTEMAP
no bgp dampening REACHTIME
no bgp dampening REACHTIME REUSE
no bgp dampening REACHTIME REUSE SUPPRESS MAXSUPPRESS (UNREACHTIME)
no bgp dampening route-map (ROUTEMAP)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>REACHTIME</td>
<td>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.</td>
<td>1-45</td>
</tr>
<tr>
<td>REUSE</td>
<td>Specifies the reuse limit value. When the penalty for a suppressed route decays below the reuse value, the routes become unsuppressed. The default reuse limit is 750 SUPPRESS &lt;1-20000&gt;. 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.</td>
<td>1-20000</td>
</tr>
<tr>
<td>SUPPRESS</td>
<td>Specifies suppress-time. A route dampening more than this value will be suppressed. The default value is 2000.</td>
<td>1-20000</td>
</tr>
<tr>
<td>MAXSUPPRESS</td>
<td>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).</td>
<td>1-255</td>
</tr>
<tr>
<td>UNREACHTIME</td>
<td>Specifies the un-reachability half-life time for penalty, in minutes.</td>
<td>1-45</td>
</tr>
<tr>
<td>ROUTEMAP</td>
<td>route-map WORD Route-map to specify criteria for dampening.</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration
Address Family Configuration

**Default**

N/A

**Usage**

Route dampening minimizes the instability caused by route flapping. A penalty is added for every flap in a flapping route. As soon as the total penalty reaches the suppress limit the advertisement of the route is suppressed. This penalty is decayed according to the configured half time value. Once the penalty is lower than the reuse limit, the route advertisement is un-suppressed. The dampening information is purged from the router once the penalty becomes less than half of the reuse limit.

**Examples**

Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp dampening 20 800 2500 80 25
Related Commands

N/A

6.7.13 bgp default ipv4-unicast

Command Purpose

Use this command to configure BGP defaults and activate ipv4-unicast for a peer by default. This affects the BGP global configuration. Use the no parameter with this command to disable this function.

Command Syntax

bgp default ipv4-unicast
no bgp default ipv4-unicast

Command Mode

Router Configuration

Default

The bgp default ipv4 unicast is the default behavior.

Usage

The no bgp default ipv4-unicast command is used to disable the default behavior of the BGP routing process of exchanging IPv4 addressing information with BGP neighbor routers.

Examples

Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp default ipv4-unicast

Related Commands

N/A
6.7.14 bgp default local-preference

Command Purpose

Use this command to change the default local preference value. Use the no parameter with this command to revert to the default setting.

Command Syntax

bgp default local-preference \textit{PREF\.VALUE}
no default local-preference ( \textit{PREF\.VALUE} )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>\textit{PREF.VALUE}</td>
<td>Configure default local preference value.</td>
<td>0\textdash 4294967295</td>
</tr>
<tr>
<td></td>
<td>The default local preference value is 100.</td>
<td></td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

The default local preference value is 100.

Usage

Local preference indicates the preferred path when there are multiple paths to the same destination. The path having a higher preference is preferred. Use bgp default local-preference command to define preference of a particular path. The preference is sent to all routers and access servers in the local autonomous system.

Examples

Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp default local-preference 2345555

Related Commands

N/A
6.7.15 bgp deterministic-med

Command Purpose

Use this command to compare the Multi Exit Discriminator (MED) variable when choosing among routes advertised by different peers in the same autonomous system.
Use the no parameter with this command to disallow this setting.

Command Syntax

bgp deterministic-med
no bgp deterministic-med

Command Mode

Router Configuration

Default

Disabled

Usage

"Multi Exit Discriminator (MED) is used in best path selection by BGP. MED is compared after BGP attributes weight, local preference, AS-path and origin have been compared and are equal. Enable bgp deterministic med command on all routers in the local AS, for a correct comparison result. After enabling this command, all paths for the same prefix are grouped together and arranged according to their MED value.
Based on this comparison, the best path is then chosen.
This command compares MED variable when choosing routes advertised by different peers in the same AS, to compare MED, when choosing routes from neighbors in different ASs use the bgp always-compare-med command."

Examples

Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp deterministic-med

Related Commands

show ip bgp, show ip bgp neighbors
6.7.16 bgp enforce-first-as

**Command Purpose**

Use this command to specify that any updates received from an external neighbor that do not have the neighbor’s configured Autonomous System (AS) at the beginning of the AS_PATH in the received update must be denied. Use the no parameter with this command to disable this feature.

**Command Syntax**

```
bgp enforce-first-as
no bgp enforce-first-as
```

**Command Mode**

Router Configuration

**Default**

Disabled

**Usage**

Enabling this feature adds to the security of the BGP network by not allowing traffic from unauthorized systems.

**Examples**

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp enforce-first-as
```

**Related Commands**

N/A

6.7.17 bgp fast-external-failover

**Command Purpose**

Use this command to reset a BGP session immediately, if the interface used for BGP connection goes down. Use the no parameter with this command to disable this feature.
**Command Syntax**

bgp fast-external-failover
no bgp fast-external-failover

**Command Mode**

Router Configuration

**Default**

Enabled

**Usage**

None

**Examples**

Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp fast-external-failover

**Related Commands**

N/A

**6.7.18 bgp log-neighbor-changes**

**Command Purpose**

Use this command to enable logging of status change messages without turning on debug bgp commands. Use the no parameter with this command to disable this feature.

**Command Syntax**

bgp log-neighbor-changes
no bgp log-neighbor-changes

**Command Mode**

Router Configuration
Default

Disabled

Usage

System implementation provides other kinds of logging services for neighbor status, for example, debug bgp fsm, debug bgp events, etc. However, these commands create a significant hit in the logging performance.

The `bgp log-neighbor-changes` command, logs the following events:

- BGP Notification Received
- Erroneous BGP Update Received
- User reset request
- Peer time-out
- Peer Closing down the session
- Interface flap
- Router ID changed
- Neighbor deleted
- Member added to peer group
- Administrative shutdown
- Remote AS changed
- RR client configuration modification
- Soft reconfiguration modification

Examples

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp log-neighbor-changes
```

Related Commands

N/A

6.7.19 bgp router-id

Command Purpose

Use this command to configure the router identifier.
Use the no parameter with this command to disable this function

Command Syntax

```
bgp router-id ROUTERID
no bgp router-id (ROUTERID |)
```
### Command Mode

#### Router Configuration

#### Address Family Configuration

### Default

In case the loopback interface is configured the router-id is set to the IP address of a loopback interface. If not, the highest IP address is the router-id.

### Usage

Use `bgp router-id` command to manually configure a fixed router ID as a BGP router identifier.

### Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp router-id 1.1.2.3
```

### Related Commands

N/A

### 6.7.20 bgp scan-time

#### Command Purpose

Use this command to set the interval for BGP route next-hop scanning.

Use the `no` parameter with this command to disable this function.

#### Command Syntax

```
bgp scan-time TIME
no bgp scan-time (TIME |)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIME</td>
<td>Scanning interval in seconds. The default scanning interval is 60 seconds.</td>
<td>0-60</td>
</tr>
</tbody>
</table>
**Command Mode**

Router Configuration

**Default**

N/A

**Usage**

Use this command to configure scanning intervals of BGP routers. This interval is the period after which router checks the validity of the routes in its database.

To disable BGP scanning, set the scan time interval to 0 seconds.

**Examples**

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp scan-time 10
```

**Related Commands**

N/A

**6.7.21 clear ip bgp * **

**Command Purpose**

Use this command to reset a BGP connection for all peers.

**Command Syntax**

```
clear ip bgp * (IN | out | SOFT |)
clear ip bgp * ipv4 PREFIX ROUTES
clear ip bgp * vpng4 unicast ROUTES
clear ip bgp * vrf NAME ROUTES
```
### Parameter | Parameter Description | Parameter Value
--- | --- | ---
* | clears all bgp peers | -
ipv4 | clears all IPv4 address family peers | -
vpnv4 | clears all vvpn4 address family peers | -
ROUTES | (IN|out|SOFT) | -
IN | in (prefix-filter) | -
.. | in | Indicates that incoming advertised routes will be cleared | -
prefix-filter | Pushes out prefix-list ORF and does inbound soft reconfiguration | -
.. | out | Indicates that outgoing advertised routes will be cleared | -
SOFT | soft (in|out) indicates that both incoming and outgoing routes will be cleared | -
PREFIX | (unicast|multicast) | -
unicast | address family modifier | -
multicast | address family modifier | -
vrf | VPN routing/forwarding instance | -
NAME | VPN Routing/Forwarding instance name | Up to 15 characters

### Command Mode
Privileged EXEC

### Default
N/A

### Usage
There are two kind BGP reset, hard reset will clear BGP peers and establish again. Soft reset only refresh routing table.

### Examples
```
Switch# clear ip bgp *
Switch# clear ip bgp * ipv4 unicast in prefix-filter
Switch# clear ip bgp * vvpn4 unicast in
```

### Related Commands
N/A
6.7.22 clear ip bgp A.B.C.D

Command Purpose

Use this command to reset a IPv4 BGP connection for a specific IP address.

Command Syntax

clear ip bgp A.B.C.D (in | out | SOFT)
clear ip bgp A.B.C.D ipv4 PREFIX ROUTES
clear ip bgp A.B.C.D vpnv4 unicast ROUTES
clear ip bgp A.B.C.D vrf NAME ROUTES

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D</td>
<td>Specifies the IPv4 address of the BGP route to be cleared</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>ipv4</td>
<td>clears all IPv4 address family peers</td>
<td>-</td>
</tr>
<tr>
<td>vpnv4</td>
<td>clears all VPNv4 address family peers</td>
<td>-</td>
</tr>
<tr>
<td>ROUTES</td>
<td>(in</td>
<td>out</td>
</tr>
<tr>
<td>IN</td>
<td>in prefix-filter</td>
<td>-</td>
</tr>
<tr>
<td>in</td>
<td>Indicates that incoming advertised routes will be cleared</td>
<td>-</td>
</tr>
<tr>
<td>prefix-filter</td>
<td>Pushes out prefix-list ORF and does inbound soft reconfiguration</td>
<td>-</td>
</tr>
<tr>
<td>out</td>
<td>Indicates that outgoing advertised routes will be cleared</td>
<td>-</td>
</tr>
<tr>
<td>SOFT</td>
<td>soft (in</td>
<td>out!) Indicates that both incoming and outgoing routes will be cleared</td>
</tr>
<tr>
<td>PREFIX</td>
<td>(unicast</td>
<td>multicast)</td>
</tr>
<tr>
<td>unicast</td>
<td>address family modifier</td>
<td>-</td>
</tr>
<tr>
<td>multicast</td>
<td>address family modifier</td>
<td>-</td>
</tr>
<tr>
<td>vrf</td>
<td>VPN routing/forwarding instance</td>
<td>-</td>
</tr>
<tr>
<td>NAME</td>
<td>VPN Routing/Forwarding instance name</td>
<td>Up to 15 characters</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A
Examples

Switch# clear ip bgp 10.10.0.12 soft
Switch# clear ip bgp 10.10.0.10 vpnv4 unicast out
Switch# clear ip bgp 11.11.11.11 ipv4 multicast in prefix-filter

Related Commands

N/A

6.7.23 clear ip bgp dampening

Command Purpose

Use this command to reset all dampened BGP routes under the specified address family.

Command Syntax

clear ip bgp dampening (A.B.C.D | A.B.C.D/M )
clear ip bgp ipv4 PREFIX dampening (A.B.C.D | A.B.C.D/M )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D</td>
<td>Specifies the IPv4 address for which Bgp dampening is to be cleared.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>A.B.C.D/M</td>
<td>Specifies the IPv4 address with mask for which Bgp dampening is to be cleared.</td>
<td>IPv4 Address and mask length in A.B.C.D/M format</td>
</tr>
<tr>
<td>ipv4</td>
<td>clears all IPv4 address family peers</td>
<td>-</td>
</tr>
<tr>
<td>PREFIX</td>
<td>(unicast</td>
<td>multicast)</td>
</tr>
<tr>
<td>unicast</td>
<td>address family modifier</td>
<td>-</td>
</tr>
<tr>
<td>multicast</td>
<td>address family modifier</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A
Examples

Switch# clear ip bgp dampening 10.10.0.121
Switch# clear ip bgp ipv4 unicast dampening

Related Commands

N/A

6.7.24 clear ip bgp flap-statistics

Command Purpose

Use this command to clear the flap count and history duration for all the prefixes under the specified address family.

Command Syntax

clear ip bgp flap-statistics (A.B.C.D | A.B.C.D/M)
clear ip bgp ipv4 PREFIX flap-statistics (A.B.C.D | A.B.C.D/M)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D</td>
<td>Specifies the IPv4 address for which Bgp dampening is to be cleared.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>A.B.C.D/M</td>
<td>Specifies the IPv4 address with mask for which Bgp dampening is to be cleared.</td>
<td>IPv4 Address and mask length in A.B.C.D/M format</td>
</tr>
<tr>
<td>ipv4</td>
<td>clears all IPv4 address family peers</td>
<td>-</td>
</tr>
<tr>
<td>PREFIX</td>
<td>(unicast</td>
<td>multicast)</td>
</tr>
<tr>
<td>unicast</td>
<td>address family modifier</td>
<td>-</td>
</tr>
<tr>
<td>multicast</td>
<td>address family modifier</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A
Examples

Switch# clear ip bgp flap-statistics 10.10.0.121
Switch# clear ip bgp ipv4 unicast flap-statistics

Related Commands

N/A

6.7.25 clear ip bgp ASN

Command Purpose

Use this command to reset a BGP connection for all peers in a specified Autonomous System.

Command Syntax

clear ip bgp ASN (IN | out | SOFT |)
clear ip bgp ASN ipv4 PREFIX ROUTES
clear ip bgp ASN vpnv4 unicast ROUTES

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASN</td>
<td>Specifies the AS Number for which all routes will be cleared</td>
<td>1-65535</td>
</tr>
<tr>
<td>ipv4</td>
<td>clears all IPv4 address family peers</td>
<td>-</td>
</tr>
<tr>
<td>vpnv4</td>
<td>clears all VPNv4 address family peers</td>
<td>-</td>
</tr>
<tr>
<td>ROUTES</td>
<td>(IN</td>
<td>out</td>
</tr>
<tr>
<td>IN</td>
<td>in prefix-filter</td>
<td>-</td>
</tr>
<tr>
<td>in</td>
<td>Indicates that incoming advertised routes will be cleared</td>
<td>-</td>
</tr>
<tr>
<td>out</td>
<td>Indicates that outgoing advertised routes will be cleared.</td>
<td>-</td>
</tr>
<tr>
<td>prefix-filter</td>
<td>Pushes out prefix-list ORF and does inbound soft reconfiguration</td>
<td>-</td>
</tr>
<tr>
<td>SOFT</td>
<td>soft (in</td>
<td>out) Indicates that both incoming and outgoing routes will be cleared</td>
</tr>
<tr>
<td>PREFIX</td>
<td>(unicast</td>
<td>multicast)</td>
</tr>
<tr>
<td>unicast</td>
<td>address family modifier</td>
<td>-</td>
</tr>
<tr>
<td>multicast</td>
<td>address family modifier</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC
Default
N/A

Usage
N/A

Examples
Switch# clear ip bgp 100
Switch# clear ip bgp 200 ipv4 unicast in prefix-filter
Switch# clear ip bgp 500 vpnv4 unicast in

Related Commands
N/A

6.7.26 clear ip bgp external

Command Purpose
Use this command to reset a BGP connection for all external peers.

Command Syntax

clear ip bgp external (in | out | SOFT |)
clear ip bgp external ipv4 PREFIX ROUTES

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>external</td>
<td>Clears all external peers</td>
<td>-</td>
</tr>
<tr>
<td>ROUTES</td>
<td>(IN</td>
<td>out</td>
</tr>
<tr>
<td>IN</td>
<td>in prefix-filter</td>
<td>-</td>
</tr>
<tr>
<td>in</td>
<td>Indicates that incoming advertised routes will be cleared</td>
<td>-</td>
</tr>
<tr>
<td>out</td>
<td>Indicates that outgoing advertised routes will be cleared.</td>
<td>-</td>
</tr>
<tr>
<td>SOFT</td>
<td>soft (in</td>
<td>out</td>
</tr>
<tr>
<td>ipv4</td>
<td>clears all IPv4 address family peers</td>
<td>-</td>
</tr>
<tr>
<td>PREFIX</td>
<td>(unicast</td>
<td>multicast)</td>
</tr>
<tr>
<td>unicast</td>
<td>address family modifier</td>
<td>-</td>
</tr>
<tr>
<td>multicast</td>
<td>address family modifier</td>
<td>-</td>
</tr>
</tbody>
</table>
**Command Mode**

Privileged EXEC

**Default**

N/A

**Usage**

N/A

**Examples**

Switch# clear ip bgp external out
Switch# clear ip bgp external ipv4 unicast in prefix-filter

**Related Commands**

N/A

6.7.27 clear ip bgp peer-group

**Command Purpose**

Use this command to reset a BGP connection for all members of a peer group.

**Command Syntax**

clear ip bgp peer-group WORD ( In | out | SOFT )
clear ip bgp peer-group WORD ipv4 PREFIX ROUTES

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer-group</td>
<td>Clears all members of a peer group</td>
<td>-</td>
</tr>
<tr>
<td>WORD</td>
<td>Specifies the name of the peer group for which all members will be cleared.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>ipv4</td>
<td>clears all IPv4 address family peers</td>
<td>-</td>
</tr>
<tr>
<td>ROUTES</td>
<td>(IN</td>
<td>out</td>
</tr>
<tr>
<td>prefix-filter</td>
<td>Pushes out prefix-list ORF and does inbound soft reconfiguration</td>
<td>-</td>
</tr>
<tr>
<td>IN</td>
<td>in prefix-filter</td>
<td>-</td>
</tr>
<tr>
<td>in</td>
<td>Indicates that incoming advertised routes will be cleared</td>
<td>-</td>
</tr>
<tr>
<td>out</td>
<td>Indicates that outgoing advertised routes will be cleared.</td>
<td>-</td>
</tr>
<tr>
<td>SOFT</td>
<td>soft (in</td>
<td>out</td>
</tr>
<tr>
<td>PREFIX</td>
<td>(unicast</td>
<td>multicast)</td>
</tr>
<tr>
<td>unicast</td>
<td>address family modifier</td>
<td>-</td>
</tr>
<tr>
<td>multicast</td>
<td>address family modifier</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC
Default

N/A

Usage

None

Examples

Switch# clear ip bgp-group Peer1 out
Switch# clear ip bgp-group mypeer ipv4 unicast in prefix-filter

Related Commands

N/A

6.7.28 clear ip bgp vrf

Command Purpose

Use this command to reset the specified VPN Routing/Forwarding Instance for BGP connections.

Command Syntax

clear ip bgp ( A.B.C.D | * ) vrf (out | in | SOFT )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>Specifies the name of the VRF</td>
<td>Up to 15 characters</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the IPv4 address of the BGP route to be cleared</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>*</td>
<td>Clears all peers</td>
<td>-</td>
</tr>
<tr>
<td>out</td>
<td>Performs soft reconfiguration out</td>
<td>-</td>
</tr>
<tr>
<td>SOFT</td>
<td>soft (in</td>
<td>out) Indicates that both incoming and outgoing routes will be cleared</td>
</tr>
<tr>
<td>in</td>
<td>Performs soft reconfiguration in</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

N/A
Usage

If the neighbor address is specified with this command it clears the specified connection. If no address is specified this command clears all the BGP routes.

Examples

Switch# clear ip bgp 3.3.3.3 vrf VRF1 soft in

Related Commands

N/A

6.7.29 debug bgp

Command Purpose

Use this command to specify all debugging options for BGP. Use the no parameter with this command to disable this function.

Command Syntax

debug bgp ( all | dampening | events | filters | fsm | keepalives | mpls | updates )
no debug bgp ( all | dampening | events | filters | fsm | keepalives | mpls | nsm | updates )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Used with the no form exclusively; turns off all debugging for BGP</td>
<td>-</td>
</tr>
<tr>
<td>dampening</td>
<td>Specifies debugging for Bgp dampening.</td>
<td>-</td>
</tr>
<tr>
<td>events</td>
<td>Specifies debugging for BGP events.</td>
<td>-</td>
</tr>
<tr>
<td>filters</td>
<td>Specifies debugging for BGP filters.</td>
<td>-</td>
</tr>
<tr>
<td>fsm</td>
<td>Specifies debugging for BGP Finite State Machine (FSM).</td>
<td>-</td>
</tr>
<tr>
<td>mpls</td>
<td>Specifies debugging for BGP Multiprotocol Label Switching.</td>
<td>-</td>
</tr>
<tr>
<td>keepalives</td>
<td>Specifies debugging for BGP keepalives.</td>
<td>-</td>
</tr>
<tr>
<td>updates</td>
<td>Specifies debugging for BGP updates.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

N/A
Usage

This command without any parameters turns on normal bgp debug information.

Examples

```
Switch# debug bgp
Switch# debug bgp events
```

Related Commands
N/A

6.7.30 distance

Command Purpose

Use this command to define an administrative distance.
Use the no parameter with this command to remove an administrative distance.

Command Syntax

```
distance ADMINDISTANCE IP_ADDR/IP_MASK_LEN
no distance ADMINDISTANCE IP_ADDR/IP_MASK_LEN
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMINDISTANCE</td>
<td>Specifies the administrative distance.</td>
<td>1-255</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>the IP source prefix</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IP_MASK_LEN</td>
<td>the IP source prefix mask length</td>
<td>1-32</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration

Default
N/A

Usage

Use this command to set the administrative distance for BGP. This distance is a rating of trustworthiness of a router.
The higher the distance the lower the trust rating.
The administrative distance can be set for external, internal and local routes. External paths are routes learned from a neighbor out of the AS. The internal routes are routes learned from another router within the same AS. Local routes are for the router that is being redistributed from another process.
If the administrative distance is changed, it could create inconsistency in the routing table and obstruct routing.
Examples

Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) distance 34 10.10.0.0/24 mylist
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) distance bgp 34 23 15

Related Commands

N/A

6.7.31  exit-address-family

Command Purpose

Use this command to exit the address family mode.

Command Syntax

exit-address-family

Command Mode

Address Family Configuration

Default

N/A

Usage

N/A

Examples

The following example shows the use of exit-address-family command and the change in the prompt after using this command:

Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# address-family ipv4 unicast
Switch(config-router-af)# exit-address-family
Switch(config-router)#
**Related Commands**

address-family

**6.7.32 ip as-path access-list**

**Command Purpose**

Use this command to define a BGP Autonomous System (AS) path access list. Use the no parameter with this command to disable use of the access list.

**Command Syntax**

```
ip as-path access-list LISTNAME (deny | permit) LINE
no ip as-path access-list LISTNAME (deny | permit) LINE
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISTNAME</td>
<td>Specifies the name of the access list.</td>
<td>Up to 40 characters, the first character must be among [a-zA-Z0-9]</td>
</tr>
<tr>
<td>deny</td>
<td>(Optional) Denies access to matching conditions.</td>
<td>-</td>
</tr>
<tr>
<td>permit</td>
<td>(Optional) Permits access to matching conditions.</td>
<td>-</td>
</tr>
<tr>
<td>LINE</td>
<td>Specifies a regular expression to match the BGP AS paths.</td>
<td>A regular expression to match the BGP AS paths</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

N/A

**Usage**

Named community list is a filter based on regular expressions. If the regular expression matches the specified string representing the AS path of the route, then the permit or deny condition applies. Use this command to define the BGP access list globally, use the neighbor router configuration command to apply a specific access list.

**Examples**

```
Switch# configure terminal
Switch(config)# ip as-path access-list mylist deny ^65535$ 
```
**6.7.33 ip community-list**

**Command Purpose**

Use this command to add a community list entry.<br>Use the no parameter with this command to delete the community list entry.

**Command Syntax**

```plaintext
ip community-list LISTNUM (deny | permit) COMMUNITY
no ip community-list LISTNUM (deny | permit) COMMUNITY
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISTNUM</td>
<td>Specifies the community ID. 1-99: Standard list 100-199: Expandes list</td>
<td>1-199</td>
</tr>
<tr>
<td>deny</td>
<td>Specifies the community to reject.</td>
<td>-</td>
</tr>
<tr>
<td>permit</td>
<td>Specifies the community to accept.</td>
<td>-</td>
</tr>
<tr>
<td>COMMUNITY</td>
<td>(AA:NN</td>
<td>internet</td>
</tr>
<tr>
<td>AA:NN</td>
<td>Specifies the valid value for the community number. This format represents the 32 bit communities value, where AS is the high order 16 bits and VAL is the low order 16 bits in digit As a format. AA is in the range 1-65535 NN is in the range of 1-65535</td>
<td>-</td>
</tr>
<tr>
<td>internet</td>
<td>Specifies routes not to be advertised to the Internet.</td>
<td>-</td>
</tr>
<tr>
<td>local-AS</td>
<td>Specifies routes not to be advertised to external BGP peers.</td>
<td>-</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Specifies routes not to be advertised to other BGP peers.</td>
<td>-</td>
</tr>
<tr>
<td>no-export</td>
<td>Specifies routes not to be advertised outside of Autonomous System boundary.</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

N/A
Usage
Use the community-lists to specify BGP community attributes. The community attribute is used for implementing policy routing. It is an optional, transitive attribute and facilitates transfer of local policies through different autonomous systems. It includes community values that are 32 bits long.

There are two kinds of community-lists: the expanded and standard. The standard community-list defines the community attributes in a specified format and not with regular expressions. The expanded community-list defines the communities attributes with regular expressions.

Examples
Switch# configure terminal
Switch(config)# ip community-list 20 permit 7675:80 7675:90

Related Command
ip community-list standard
ip community-list expanded

6.7.34 ip community-list expanded

Command Purpose
Use this command to add a community list entry.
Use the no parameter with this command to delete the community list entry.

Command Syntax
ip community-list expanded WORD ( deny | permit ) LINE
no ip community-list expanded WORD ( deny | permit ) LINE

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>expanded</td>
<td>Add an expanded community-list entry.</td>
<td>-</td>
</tr>
<tr>
<td>WORD</td>
<td>Expanded community list name</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>deny</td>
<td>Specifies community to reject.</td>
<td>-</td>
</tr>
<tr>
<td>permit</td>
<td>Specifies community to accept.</td>
<td>-</td>
</tr>
<tr>
<td>LINE</td>
<td>Specifies a regular expression to match the</td>
<td>A regular expression</td>
</tr>
<tr>
<td></td>
<td>BGP AS paths.</td>
<td></td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
N/A
Usage
Use the community-lists to specify BGP community attributes. The community attribute is used for implementing policy routing. It is an optional, transitive attribute and facilitates transfer of local policies through different autonomous systems. It includes community values that are 32 bits long.
There are two kinds of community-lists – the expanded and standard. The standard community-list defines the community attributes in a specified format and not with regular expressions. The expanded community-list defines the communities attributes with regular expressions.

Examples
Switch# configure terminal
Switch(config)# ip community-list expanded CLIST permit.*

Related Commands
ip community-list
ip community-list standard

6.7.35 ip community-list standard

Command Purpose
Use this command to add a standard community-list entry.
Use the no parameter with this command to delete the standard community-list entry.

Command Syntax
ip community-list standard WORD (deny | permit) COMMUNITY
no ip community-list standard WORD (deny | permit) COMMUNITY

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>standard</td>
<td>Specifies a standard community list.</td>
<td>-</td>
</tr>
<tr>
<td>WORD</td>
<td>Standard community list name</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>deny</td>
<td>Specifies community to reject.</td>
<td>-</td>
</tr>
<tr>
<td>permit</td>
<td>Specifies community to accept.</td>
<td>-</td>
</tr>
<tr>
<td>COMMUNITY</td>
<td>(AA:NN</td>
<td>internet</td>
</tr>
<tr>
<td>AA: NN</td>
<td>Specifies the valid value for the community number. This format represents the 32 bit communities value, where AS is the high order 16 bits and VAL is the low order 16 bits in digit.</td>
<td>AA is in the range 1-65535 NN is in the range of 1-65535</td>
</tr>
<tr>
<td>internet</td>
<td>Specifies routes not to be advertised to the Internet.</td>
<td>-</td>
</tr>
<tr>
<td>local-AS</td>
<td>Specifies routes not to be advertised to external BGP peers.</td>
<td>-</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Specifies routes not to be advertised to other BGP peers.</td>
<td>-</td>
</tr>
<tr>
<td>no-export</td>
<td>Specifies routes not to be advertised outside of the Autonomous System boundary.</td>
<td>-</td>
</tr>
</tbody>
</table>
Command Mode

Global Configuration

Default

N/A

Usage

Use the community-lists to specify BGP community attributes. The community attribute is used for implementing policy routing. It is an optional, transitive attribute and facilitates transfer of local policies through different autonomous systems. It includes community values that are 32 bits long.

There are two kinds of community-lists – the expanded and standard. The standard community-list defines the community attributes in a specified format without regular expressions. The expanded community-list defines the communities attributes with regular expressions.

Use the ip community-list standard command to add a standard community-list entry. The standard community-list is compiled into binary format and is directly compared with the BGP communities attribute in the BGP updates. The comparison is faster than the expanded community-list. Any community value that does not match the standard community value is automatically treated as expanded.

Examples

Switch# configure terminal
Switch(config)# ip community-list standard CLIST permit 7675:80 7675:90 no-export

Related Commands

ip community-list
ip community-list expanded

6.7.36 neighbor activate

Command Purpose

Use this command to enable the exchange of the specified AF routes with a neighboring router.

Use the no parameter with this command to disable exchange of information with a neighbor.

Command Syntax

neighbor NEIGHBORID activate
no neighbor NEIGHBORID activate
### Parameter Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D)[TAG]</td>
<td>-</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

#### Command Mode

Router Configuration
Address Family Configuration

#### Default

N/A

#### Usage

After the TCP connection is opened with the neighbor, this command is used to enable or disable the exchange of the specified AF information with a neighboring router.
To enable the exchange of multicast and VPNv4 address prefix types, neighbors are activated using the neighbor activate command in address family mode.

#### Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 1.2.3.4 activate
```

#### Related Commands

neighbor remote-as

6.7.37 neighbor advertisement-interval

#### Command Purpose

Use this command to set the minimum interval between sending the BGP routing updates.
Use the no parameter with this command to set the interval time to default.
Command Syntax

neighbor NEIGHBORID advertisement-interval TIME
no neighbor NEIGHBORID advertisement-interval TIME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D)[TAG]</td>
<td>-</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>TIME</td>
<td>Advertise -interval value in seconds</td>
<td>0-600</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

N/A

Usage

Use this command to set the minimum interval between the sending of BGP routing updates. To reduce the flapping of routes to internet, a minimum advertisement interval is set, so that the BGP routing updates are sent only per interval seconds. bgp dampening can also be used to control the effects of flapping routes. For the originated bgp routes, they would be sent out when as-origination-interval and advertisement-interval expired at the same time.

Examples

Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.3 advertisement-interval 45

Related Commands

N/A

6.7.38 neighbor as-origination-interval

Command Purpose

Use this command to set the minimum interval between ready to send the originated BGP routing updates.
Use the no parameter with this command to set the interval time to default.
Command Syntax

neighbor NEIGHBORID as-origination-interval TIME
no neighbor NEIGHBORID as-origination-interval TIME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D)[TAG]</td>
<td>-</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>TIME</td>
<td>Advertise interval value in seconds</td>
<td>0-600</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default
N/A

Usage

Use this command to set the minimum interval between the ready to send of originated BGP routing updates. For the originated bgp routes, they would be sent out when as-origination-interval and advertisement-interval expired at the same time.

Examples

Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.3 advertisement-interval 45

Related Commands
N/A

6.7.39 neighbor allowas-in

Command Purpose

Use this command to configure PE routers to allow re-advertisement of all prefixes containing duplicate Autonomous System Numbers (ASNs).

Use the no parameter with this command to disable the readvertisement of a PE router’s ASN.
Command Syntax

neighbor NEIGHBOR allowas-in [ NUMBER ]
no neighbor NEIGHBOR allowas-in

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D</td>
<td>TAG)</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>NUMBER</td>
<td>Number of occurrences of AS number. Default value is 1</td>
<td>1-10</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration
Address Family Configuration

Default
Disabled

Usage
In a hub and spoke configuration, a PE router re-advertises all prefixes containing duplicate ASNs. Use the neighbor allowas-in command to configure two VRFs on each PE router to receive and re-advertise prefixes. One of the VRFs receives prefixes with ASNs from all PE routers and then advertises them to neighboring PE routers. The other VRF receives prefixes with ASNs from the CE router and re-advertises them to all PE routers in the hub and spoke configuration.

Control the number of times an ASN is advertised, by specifying a number from 1 to 10.

Examples
Switch(config-router)# configure terminal
Switch(config-router)# address-family ipv4 vrf VRF_A
Switch(config-router-af)# neighbor 10.10.0.1 allowas-in 3

Related Commands
N/A
6.7.40 neighbor attribute-unchanged

Command Purpose

Use this command to advertise unchanged BGP attributes to the specified neighbor. Use the no parameter with this command to disable this function.

Command Syntax
neighbor NEIGHBORID attribute-unchanged { as-path | next-hop | med }
no neighbor NEIGHBORID attribute-unchanged { as-path | next-hop | med }

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D)[TAG]</td>
<td>-</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>as-path</td>
<td>AS path attribute</td>
<td>-</td>
</tr>
<tr>
<td>next-hop</td>
<td>Next hop attribute</td>
<td>-</td>
</tr>
<tr>
<td>med</td>
<td>Multi Exit Discriminator</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration
Address Family Configuration

Default
N/A

Usage
N/A

Examples
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.75 attribute-unchanged as-path med

Related Commands
N/A
6.7.41 neighbor capability dynamic

Command Purpose

Use this command to enable the dynamic capability for a specific peer.
Use the no parameter with this command to disable the dynamic capability.

Command Syntax

neighbor NEIGHBORID capability dynamic
no neighbor NEIGHBORID capability dynamic

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D</td>
<td>TAG)</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

Disabled

Usage

This command allows a BGP speaker to advertise or withdraw an address family capability to a peer in a non-disruptive manner.

Examples

Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.10.1 capability dynamic

Related Commands

N/A
### 6.7.42 neighbor capability orf prefix-list

**Command Purpose**

Use this command to advertise ORF capability to neighbors.

Use the no parameter with this command to disable this function.

**Command Syntax**

```
neighbor NEIGHBORID capability orf prefix-list (both | receive | send)
no neighbor NEIGHBORID capability orf prefix-list (both | receive | send)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D)(TAG)</td>
<td>-</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>orf</td>
<td>Advertises ORF capability to its neighbors</td>
<td>-</td>
</tr>
<tr>
<td>both</td>
<td>Indicates that the local router can send ORF entries to its peer as well as receive ORF entries from its peer.</td>
<td>-</td>
</tr>
<tr>
<td>receive</td>
<td>Indicates that the local router is willing to receive ORF entries from its peer</td>
<td>-</td>
</tr>
<tr>
<td>send</td>
<td>Indicates that the local router is willing to send ORF entries to its peer</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

- Router Configuration
- Address Family Configuration

**Default**

N/A

**Usage**

Outbound Route Filters (ORFs) send and receive capabilities to lessen the number of updates exchanged between neighbors. By filtering updates, this option minimizes generating and processing of updates.

The local router advertises the ORF capability in send mode and the remote router receives the ORF capability in receive mode applying the filter as outbound policy. The two routers exchange updates to maintain the ORF for each

**Examples**

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 1.1.1.1 capability orf prefix-list both
```
Related Commands

N/A

6.7.A3 neighbor capability route-refresh

Command Purpose

Use this command to advertise route-refresh capability to the specified neighbors.
Use the no parameter with this command to disable this function.

Command Syntax

neighbor NEIGHBORID capability route-refresh
no neighbor NEIGHBORID capability route-refresh

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format. IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group. Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

N/A

Usage

Use this command to advertise to peer about route refresh capability support. If route refresh capability is supported, then router can dynamically request that the peer readvertises its Adj-RIB-Out.

Examples

Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.10.1 capability route-refresh
Related Commands
N/A

6.7.44 neighbor default-originate

Command Purpose
Use this command to allow a BGP local router to send the default route 0.0.0.0 to a neighbor for use as a default route. Use the no parameter with this command to send no route as a default.

Command Syntax
neighbor NEIGHBORID default-originate (ROUTEMAP | )
no neighbor NEIGHBORID default-originate (ROUTEMAP | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D</td>
<td>TAG)</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>ROUTEMAP</td>
<td>route-map WORD</td>
<td>-</td>
</tr>
<tr>
<td>route-map</td>
<td>The route-map to specify criteria to originate default routes</td>
<td>-</td>
</tr>
<tr>
<td>WORD</td>
<td>Route-map name</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration
Address Family Configuration

Default
N/A

Usage
Every router should have a default route, it is used to send datas to the network which is not existent in local RIB. To set a default route on each router can make every router have a default route, or to create a default route and broadcast it to BGP peer by this command.

Examples
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.10.1 default-originate route-map myroute

Related Commands
N/A
6.7.45 neighbor description

Command Purpose

Use this command to associate a description with a neighbor.
Use the no parameter with this command to remove the description.

Command Syntax

neighbor NEIGHBORID description LINE
no neighbor NEIGHBORID description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D</td>
<td>TAG)</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>LINE</td>
<td>A string to describing the neighbor.</td>
<td>Up to 80 characters</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration
Address Family Configuration

Default

N/A

Usage

None

Examples

Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 1.2.3.4 description Backup router for sales.

Related Commands

N/A
6.7.46 neighbor distribute-list

Command Purpose

Use this command to filter route update from a particular BGP neighbor.
Use the no parameter with this command to remove an entry.

Command Syntax

neighbor NEIGHBORID distribute-list WORD (in | out)
no neighbor NEIGHBORID distribute-list WORD (in | out)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D</td>
<td>TAG)</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>WORD</td>
<td>The name of IP access-list</td>
<td>Up to 40 characters</td>
</tr>
<tr>
<td>in</td>
<td>Indicates that incoming advertised routes will be filtered.</td>
<td>-</td>
</tr>
<tr>
<td>out</td>
<td>Indicates that outgoing advertised routes will be filtered.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration
Address Family Configuration

Default

N/A

Usage

Use only one distribute-list per BGP neighbor.

Examples

Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 1.2.3.4 distribute-list mylist out
6.7.47 neighbor ebgp-multihop

Command Purpose

Use this command to accept and attempt BGP connections to external peers on indirectly connected networks. Use the no parameter with this command to return to the default.

Command Syntax

neighbor NEIGHBORID ebgp-multihop (COUNT)
noneighbor NEIGHBORID ebgp-multihop

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D</td>
<td>TAG)</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>COUNT</td>
<td>Maximum hop count. If the maximum hop count is not set the hop count is 255.</td>
<td>1-255</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

N/A

Usage

Multihop is not established if the only route to the multihop peer is a default route. This avoids loop formation.

Examples

Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.10.34 remote-as 20
Switch(config-router)# neighbor 10.10.10.34 ebgp-multihop 5

Related Commands

N/A
6.7.48 neighbor filter-list

Command Purpose
Use this command to set up a BGP filter.
Use the no parameter with this command to disable this function.

Command Syntax

neighbor NEIGHBORID filter-list LISTNAME (in | out)
no neighbor NEIGHBORID filter-list LISTNAME (in | out)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D</td>
<td>TAG)</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td></td>
<td>create peer groups, refer to the neighbor peer-group and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>neighbor remote-as commands. When this parameter is used</td>
<td></td>
</tr>
<tr>
<td></td>
<td>with a command, the command applies on all peers in the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>specified group.</td>
<td></td>
</tr>
<tr>
<td>in</td>
<td>Indicates that incoming advertised routes will be filtered.</td>
<td>-</td>
</tr>
<tr>
<td>out</td>
<td>Indicates that outgoing advertised routes will be filtered.</td>
<td>-</td>
</tr>
<tr>
<td>LISTNAME</td>
<td>The name of an autonomous system path access list.</td>
<td>Up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration
Address Family Configuration

Default
N/A

Usage
This command specifies an access list filter on updates based on the BGP autonomous system paths. Each filter is an access list based on regular expressions.

Examples
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.34 filter-list listname out

Related Commands
N/A
### 6.7.49 neighbor maximum-prefix

**Command Purpose**

Use this command to control the number of prefixes that can be received from a neighbor. Use the no parameter with this command to disable this function.

**Command Syntax**

```
neighbor NEIGHBORID maximum-prefix MAXIMUM
no neighbor NEIGHBORID maximum-prefix
```

**Parameter Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D</td>
<td>TAG)</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>MAXIMUM</td>
<td>MAXPREFIX (THRESHOLD</td>
<td>warning-only)</td>
</tr>
<tr>
<td>MAXPREFIX</td>
<td>Specifies the maximum number of prefixes permitted.</td>
<td>1-4294967295</td>
</tr>
<tr>
<td>THRESHOLD</td>
<td>&lt;1-100&gt; Specifies the threshold value, 1 to 100 percent.</td>
<td>1-100</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration
Address Family Configuration

**Default**

N/A

**Usage**

The neighbor maximum-prefix command allows the configuration of a specified number of prefixes that a BGP router is allowed to receive from a neighbor. When the warning-only option is not used, if any extra prefixes are received, the router ends the peering. A terminated peer, stays down until the clear ip bgp command is used.
Examples

Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.72 maximum-prefix 1244 warning-only

Related Commands

N/A

6.7.50 neighbor next-hop-self

Command Purpose

Use this command to configure the router as the next hop for a BGP-speaking neighbor or peer group. Use the no parameter with this command to disable this feature.

Command Syntax

neighbor NEIGHBORID next-hop-self
no neighbor NEIGHBORID next-hop-self

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D</td>
<td>TAG)</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration
Address Family Configuration

Default

N/A

Usage

This command allows a BGP router to change the nexthop information that is sent to the iBGP peer. The nexthop information is set to the IP address of the interface used to communicate with the neighbor.
Examples

Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.72 remote-as 100
Switch(config-router)# neighbor 10.10.0.72 next-hop-self

Related Commands

N/A

6.7.51 neighbor override-capability

Command Purpose

Use this command to override a capability negotiation result.
Use the no parameter with this command to disable this function

Command Syntax

neighbor NEIGHBORID override-capability
no neighbor NEIGHBORID override-capability

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D)TAG</td>
<td>-</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

N/A

Usage

None
Examples
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# neighbor 10.10.10.10 override-capability

Related Commands
N/A

6.7.52 neighbor passive

Command Purpose

Use this command to set a BGP neighbor as passive.
Use the no parameter with this command to disable this function

Command Syntax

( no ) neighbor NEIGHBORID passive

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D</td>
<td>TAG)</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration

Default
N/A

Usage
N/A

Examples
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# neighbor 10.10.10.10 passive

Related Commands
N/A
6.7.53 neighbor peer-group (adding a neighbor)

Command Purpose

Use this command to add a neighbor to an existing peer-group.

Use the no parameter with this command to disable this function.

Command Syntax

neighbor IPADDRESS peer-group TAG
no neighbor IPADDRESS peer-group

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPADDRESS</td>
<td>A.B.C.D Specifies the address of the BGP neighbor in IPv4 format. A.B.C.D Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of the peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

N/A

Usage

Use this command to Neighbors with the same update policies are grouped into peer groups. This facilitates the updates of various policies, such as, distribute and filter lists. The peer-group is then configured easily with any of the neighbor commands. Any changes made to the peer group affect all members.

To create a peer-group use the neighbor peer-group create command and then use this command to add neighbors to the group.

Examples

This example shows a new peer-group group1 and the adding of a neighbor 10.10.0.63 to the group:

Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor group1 peer-group
Switch(config-router)# neighbor 10.10.0.63 peer-group group1
Related Commands

N/A

6.7.54  neighbor peer-group (creating a peer-group)

Command Purpose

Use this command to create a peer-group.
Use the no parameter with this command to disable this function

Command Syntax

neighbor TAG peer-group
no neighbor TAG peer-group

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TAG</td>
<td>Name of the peer-group</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

N/A

Usage

Neighbors with the same update policies are grouped into peer groups. This facilitates the updates of various policies, such as, distribute and filter lists. The peer-group is then configured easily with any of the neighbor commands. Any changes made to the peer group affect all members. Use this command to create a peer-group.

Examples

Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor group1 peer-group

Related Commands

N/A
### 6.7.55 neighbor prefix-list

#### Command Purpose

Use this command to distribute BGP neighbor information as specified in a prefix list.

Use the no parameter with this command to remove an entry.

#### Command Syntax

neighbor NEIGHBORID prefix-list LISTNAME (in | out)

no neighbor NEIGHBORID prefix-list LISTNAME (in | out)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D</td>
<td>TAG)</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>LISTNAME</td>
<td>The number of an AS-path access list.</td>
<td>Up to 40 characters</td>
</tr>
<tr>
<td>in</td>
<td>Specifies that the access list applies to incoming advertisements.</td>
<td>-</td>
</tr>
<tr>
<td>out</td>
<td>Specifies that the access list applies to outgoing advertisements.</td>
<td>-</td>
</tr>
</tbody>
</table>

#### Command Mode

- **Router Configuration**
- **Address Family Configuration**

#### Default

N/A

#### Usage

Use this command to specify a prefix list for filtering BGP advertisements. Filtering by prefix list matches the prefixes of routes with those listed in the prefix list. If there is a match, the route is used. An empty prefix list permits all prefixes. If a given prefix does not match any entries of a prefix list, the route is denied access. When multiple entries of a prefix list match a prefix, the entry with the smallest sequence number is considered to be a real match.

The router begins the search at the top of the prefix list, with the sequence number 1. Once a match or deny occurs, the router does not need to go through the rest of the prefix list. For efficiency the most common matches or deny entries are listed at the top.

The neighbor distribute-list command is an alternative to the neighbor prefix-list command and only one of them can be used for filtering to the same neighbor in any direction.
Examples

Switch# configure terminal
Switch(config)# ip prefix-list list1 deny 30.0.0.0/24
Switch(config)# router bgp 12
Switch(config-router)# neighbor 10.10.10 prefix-list list1 in

Related Commands

ip prefix-list

6.7.56 neighbor remote-as

Command Purpose

Use this command to configure an internal or external BGP (iBGP or eBGP) TCP session with another router.

Command Syntax

neighbor NEIGHBORID remote-as ASNUM
no neighbor NEIGHBORID remote-as ASNUM

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D)TAG</td>
<td>-</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td></td>
<td>create peer groups, refer to the neighbor peer-group and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>neighbor remote-as commands. When this parameter is used</td>
<td></td>
</tr>
<tr>
<td></td>
<td>with a command, the command applies on all peers in the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>specified group.</td>
<td></td>
</tr>
<tr>
<td>ASNUM</td>
<td>Neighbor's autonomous system number</td>
<td>1-4294967295</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

N/A

Usage

This command is used to configure iBGP and eBGP sessions with other neighbors. A peer-group support of this command is configured only after creating a specific peer-group.
**Examples**

Switch# configure terminal  
Switch(config)# router bgp 11  
Switch(config-router)# neighbor 10.10.0.73 remote-as 345

**Related Commands**

N/A

**6.7.57 neighbor remove-private-AS**

**Command Purpose**

Use this command to remove the private Autonomous System (AS) number from outbound updates. Use the no parameter with this command too revert to default.

**Command Syntax**

```
neighbor NEIGHBORID remove-private-AS  
no neighbor NEIGHBORID remove-private-AS
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D)</td>
<td>TAG</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
</tbody>
</table>

**TAG**

Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group. Up to 20 characters

**Command Mode**

Router Configuration  
Address Family Configuration

**Default**

Disabled
Usage

The private AS numbers range from <64512-65535>. Private AS numbers are not advertised to the Internet. This command is used with external BGP peers only. The router removes the AS numbers only if the update includes private AS numbers. If the update includes both private and public AS numbers, the system treats it as an error.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.63 remove-private-AS
```

Related Commands

N/A

6.7.58  neighbor route-reflector-client

Command Purpose

Use this command to configure the router as a BGP route reflector and configure the specified neighbor as its client.

Use the no parameter with this command to indicate that the neighbor is not a client.

Command Syntax

```
neighbor NEIGHBORID route-reflector-client
no neighbor NEIGHBORID route-reflector-client
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D</td>
<td>TAG)</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration
Address Family Configuration

Default

N/A
Usage

Route reflectors are a solution for the explosion of iBGP peering within an autonomous system. By route reflection the number of iBGP peers within an AS is reduced. Use the neighbor route-reflector-client command to configure the local router as the route reflector and specify neighbors as its client.

An AS can have more than one route reflector. One route reflector treats the other route reflector as another iBGP speaker.

Examples

Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.72 route-reflector-client

Related Commands

N/A

6.7.59 neighbor send-community

Command Purpose

Use this command to specify that a community attribute should be sent to a BGP neighbor.

Use the no parameter with this command to remove the entry. Use the extended and no parameters to remove extended communities. Specifying no other parameter means standard communities only.

Command Syntax

neighbor NEIGHBORID send-community ( both | extended | standard )
no neighbor NEIGHBORID send-community ( both | extended | standard )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D</td>
<td>TAG)</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>both</td>
<td>Sends Standard and Extended Community attributes</td>
<td>-</td>
</tr>
<tr>
<td>extended</td>
<td>Sends Extended Community attributes</td>
<td>-</td>
</tr>
<tr>
<td>standard</td>
<td>Sends Standard Community attributes</td>
<td>-</td>
</tr>
</tbody>
</table>
**Command Mode**
Router Configuration
Address Family Configuration

**Default**
None

**Usage**
By default, community attributes are not sent to a neighbor. To use this command to enable this command. Route-map can be based on neighbor address, peer group name or AS path information.

**Examples**
Switch# configure terminal
Switch(config)# bgp config-type standard
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.72 send-community extended

**Related Commands**
N/A

**6.7.60 neighbor shutdown**

**Command Purpose**
Use this command to disable a neighbor.
Use the no parameter with this command to re-enable the neighbor.

**Command Syntax**
neighbor NEIGHBORID shutdown
no neighbor NEIGHBORID shutdown

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D</td>
<td>TAG)</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

**Command Mode**
Router Configuration

**Default**
N/A
Usage

This command shuts down any active session for the specified neighbor and clears all related routing data.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.72 shutdown
```

Related Commands

N/A

6.7.61 neighbor soft-reconfiguration inbound

Command Purpose

Use this command to configure to start storing updates.
Use the no parameter with this command to disable this function.

Command Syntax

```
neighbor NEIGHBORID soft-reconfiguration inbound
```

```
bo neighbor NEIGHBORID soft-reconfiguration inbound
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D</td>
<td>TAG)</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>create peer groups, refer to the neighbor peer-group and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>neighbor remote-as commands. When this parameter is used</td>
<td></td>
</tr>
<tr>
<td></td>
<td>with a command, the command applies on all peers in the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>specified group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration
Address Family Configuration

Default

N/A
Usage

Use this command to store updates for inbound soft reconfiguration. Soft-reconfiguration may be used in lieu of BGP route refresh capability. Using this command enables local storage of all the received routes and their attributes. This requires additional memory. When a soft reset (inbound) is done on this neighbor, the locally stored routes are reprocessed according to the inbound policy. The BGP neighbor connection is not affected.

Examples

Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# neighbor 10.10.10.10 soft-reconfiguration inbound

Related Commands

N/A

6.7.62 neighbor strict-capability-match

Command Purpose

Use this command to close the BGP connection if capability value does not completely match to remote peer. Use the no parameter with this command to disable this function

Command Syntax

neighbor NEIGHBORID strict-capability-match
no neighbor NEIGHBORID strict-capability-match

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D</td>
<td>TAG)</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

N/A
Usage

N/A

Examples

Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# neighbor 10.10.10.10 strict-capability-match

Related Commands

N/A

6.7.63 neighbor timers

Command Purpose

Use this command to set the timers for a specific BGP neighbor.
Use the no parameter with this command to clear the timers for a specific BGP neighbor

Command Syntax

neighbor NEIGHBORID timers KEEPALIVE HOLDTIME
no neighbor NEIGHBORID timers

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D</td>
<td>TAG)</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>KEEPALIVE</td>
<td>Hold time Frequency (in seconds) at which a router sends keepalive messages to its neighbor. The default is 60 seconds.</td>
<td>1-65535</td>
</tr>
<tr>
<td>HOLDTIME</td>
<td>Interval (in seconds) after which, on not receiving a keepalive message, the router declares a neighbor dead. The default is 180 seconds.</td>
<td>3-65535</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration
Default

N/A

Usage

Keepalive messages are sent by a router to inform another router that the BGP connection between the two is still active. The keepalive interval is the period of time between each keepalive message sent by the router. The holdtime interval is the time the router waits to receive a keepalive message and if it does not receive a message for this period it declares the neighbor dead.

Examples

Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# neighbor 10.10.10.10 timers 60 120

Related Commands

N/A

6.7.64 neighbor unsuppress-map

Command Purpose

Use this command to selectively leak more-specific routes to a particular neighbor.

Command Syntax

neighbor NEIGHBORID unsuppress-map WORD
no neighbor NEIGHBORID unsuppress-map WORD

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D</td>
<td>TAG)</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>WORD</td>
<td>Name of route map</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration
Address Family Configuration
Default
N/A

Usage
When the aggregate-address command is used with the summary-only option, the more-specific routes of the aggregate are suppressed to all neighbors. Use the unsuppress-map command to selectively leak more-specific routes to a particular neighbor.

Examples
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router) neighbor 10.10.0.73 unsuppress-map mymap
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router) address-family ipv4 unicast
Switch(config-router-af)neighbor 10.10.0.70 unsuppress-map mymap

Related Commands
N/A

6.7.65 neighbor update-source

Command Purpose
Use this command to allow internal BGP sessions to use any operational interface for TCP connections. Use the no parameter with this command to restore the interface assignment to the closest interface.

Command Syntax
neighbor NEIGHBORID update-source IFNAME
no neighbor NEIGHBORID update-source

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D</td>
<td>TAG)</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Specifies the loopback interface.</td>
<td>Support physical/aggregation/loop back/tunnel/vlan interfaces</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration

Default
N/A
Usage

Use this command in conjunction with any specified interface on the router. The loopback interface is the interface that is most commonly used with this command. The use of loopback interface eliminates a dependency and BGP does not have to rely on the availability of a particular interface for making TCP connections.

Examples

```bash
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.72 update-source eth-0-1
```

Related Commands

N/A

6.7.66 neighbor weight

Command Purpose

Use this command to set default weights for routes from this neighbor.
Use the no parameter with this command to remove a weight assignment.

Command Syntax

```
neighbor NEIGHBORID weight WEIGHT
no neighbor NEIGHBORID weight
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D)[TAG]</td>
<td>-</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>WEIGHT</td>
<td>Specifies the weight this command assigns to the route.</td>
<td>0-65535</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

N/A
**Usage**

Use this command to specify a weight value to all routes learned from a neighbor. The route with the highest weight gets preference when there are other routes on the network.

Unlike the local-preference attribute, the weight attribute is relevant only to the local router.

The weights assigned using the set weight command overrides the weights assigned using this command.

**Examples**

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# neighbor 10.10.10.10 weight 60
```

**Related Commands**

N/A

**6.7.67 neighbor fall-over bfd**

**Command Purpose**

Use this command to establish BFD session on BGP neighbour.

Use the no parameter with this command to delete BFD session on BGP neighbour.

**Command Syntax**

```
neighbor A.B.C.D fall-over bfd
no neighbor A.B.C.D fall-over bfd
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration

**Default**

N/A

**Usage**

Enabling bfd on bgp neighbor.
Examples

Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# neighbor 10.10.10.10 fall-over bfd

Related Commands

6.7.68 network

Command Purpose

Use this command to specify the networks to be advertised by the BGP routing process. A unicast network address without a mask is accepted if it falls into the natural boundary of its class. A class-boundary mask is derived if the address matches its natural class-boundary.

Use the no form of this command to remove a network route entry.

Command Syntax

network A.B.C.D
network A.B.C.D route-map WORD
no network A.B.C.D
no network A.B.C.D route-map WORD

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D</td>
<td>IP prefix &lt;network&gt;, e.g., 35.0.0.0</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>WORD</td>
<td>Name of the route map</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration
Address Family Configuration

Default

N/A

Usage

N/A
Examples

The following example illustrates a Class-A address configured as a network route. The natural Class-A network prefix mask length of 8 will be internally derived, that is, 2.0.0.0/8:

```
Switch# configure terminal
Switch(config)# router bgp 1
Switch(config-router)# network 2.0.0.0
```

```
!
router bgp 1
no synchronization
network 2.0.0.0
```

Related Commands

N/A

6.7.69 network synchronization

Command Purpose

Use this command to ensure the exact same static network prefix, specified through any of the network commands, is local or has IGP reachability (in the NSM RIB) before being introduced into the BGP RIB. Use the no parameter with this command to disable this function.

Command Syntax

```
network synchronization
no network synchronization
```

Command Mode

- Router Configuration
- Address Family Configuration

Default

Network synchronization is disabled by default.

Usage

N/A
### Examples
The following example enables IGP synchronization of BGP static network routes in the router configuration mode:

```
Switch# configure terminal
Switch(config)# router bgp 11
Switch(config-router)# network synchronization
```

### Related Commands
N/A

#### 6.7.70 synchronization

### Command Purpose
Use this command to enable IGP synchronization of Internal BGP (iBGP) learned routes with the Internal Gateway Protocol (IGP) system in the router configuration mode or in the address-family configuration mode.

Use the no parameter with this command to disable this function.

### Command Syntax
```
synchronization
no synchronization
```

### Command Mode
- Router Configuration
- Address Family Configuration

### Default
IGP synchronization is disabled.

### Usage
Synchronization is used when a BGP router should not advertise routes learned from iBGP neighbors, unless those routes are also present in an IGP (for example, OSPF). Synchronization may be enabled when all the routers in an autonomous system do not speak BGP, and the autonomous system is a transit for other autonomous systems. The no synchronization command is used when BGP router can advertise routes learned from its iBGP neighbors without waiting for the IGP reachability to be present.

### Examples
The following example enables IGP synchronization of BGP static network routes in the IPv4-Unicast address family:

```
Switch# configure terminal
Switch(config)# router bgp 11
Switch(config)# address-family ipv4 unicast
Switch(config-af)# network synchronization
```

### Related Commands
N/A
6.7.71  router bgp

Command Purpose

Use this command to configure a BGP routing process.
Use the no parameter with this command to disable a routing process.

Command Syntax

router bgp ASN
no router bgp ASN

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASN</td>
<td>Specifies the Autonomous System (AS) number</td>
<td>1-4294967295</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

N/A

Usage

The router bgp command enables a BGP routing process.

Examples

Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)#

Related Commands

N/A

6.7.72  show debugging bgp

Command Purpose

Use this command to display the BGP debugging option set.
### Command Syntax

`show debugging bgp`

### Command Mode

Privileged EXEC

### Default

N/A

### Usage

None

### Examples

Switch# show debugging bgp

### Related Commands

N/A

#### 6.7.73  show ip bgp

### Command Purpose

Use this command to display BGP network information.

### Command Syntax

`show ip bgp (IPADDRESS |)`

`show ip bgp ipv4 PREFIX (IPADDRESS |)`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPADDRESS</td>
<td>A.B.C.D</td>
<td>A.B.C.D/M Specifies the address and length. IPv4 Address in A.B.C.D format or IPv4 Address and mask length in A.B.C.D/M format</td>
</tr>
<tr>
<td>ipv4</td>
<td>Specifies the address family. The type of address family determines the routing table that is specified.</td>
<td>-</td>
</tr>
<tr>
<td>PREFIX</td>
<td>(multicast</td>
<td>unicast)</td>
</tr>
<tr>
<td>unicast</td>
<td>Specifies a IPv4 unicast address family. This is the default option.</td>
<td>-</td>
</tr>
<tr>
<td>multicast</td>
<td>Specifies a IPv4 multicast address family.</td>
<td>-</td>
</tr>
</tbody>
</table>

### Command Mode

Privileged EXEC

### Default

N/A
Usage
N/A

Examples
Switch# show ip bgp 10.10.1.34/24

Related Command
N/A

6.7.74 show ip bgp attribute-info

Command Purpose
Use this command to show bgp attribute information.

Command Syntax
show ip bgp attribute-info

Command Mode
Privileged EXEC

Default
N/A

Usage
N/A

Examples
This is a sample output from the show ip bgp attribute-info command displaying internal attribute information:
Switch# show ip bgp attribute-info

Related Commands
N/A

6.7.75 show ip bgp cidr-only

Command Purpose
Use this command to display routes with non-natural network masks.

Command Syntax
show ip bgp cidr-only
show ip bgp ipv4 PREFIX cidr-only
### Command Mode

Privileged EXEC

### Default

N/A

### Usage

N/A

### Examples

This is a sample output from the show ip bgp cidr-only command:

```
Switch# show ip bgp cidr-only
```

### Related Commands

N/A

### 6.7.76 show ip bgp community

#### Command Purpose

Use this command to display routes matching the communities.

#### Command Syntax

```
show ip bgp community TYPE ( exact-match | )
show ip bgp ipv4 PREFIX community TYPE ( exact-match | )
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TYPE</td>
<td>AA:NN</td>
<td>local-AS</td>
</tr>
<tr>
<td>AA:NN</td>
<td>Specifies the valid value for the community number. This format represents the 32 bit communities value, where AS is the high order 16 bits and VAL is the low order 16 bits in digit format.</td>
<td>AA is in the range 1-65535 NN is in the range of 1-65535</td>
</tr>
<tr>
<td>local-AS</td>
<td>Do not send outside local AS (well-known community).</td>
<td>-</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Do not advertise to any peer (well-known community).</td>
<td>-</td>
</tr>
<tr>
<td>no-export</td>
<td>Do not export to next AS (well-known community).</td>
<td>-</td>
</tr>
<tr>
<td>exact-match</td>
<td>Specifies that display the exact match of the communities.</td>
<td>-</td>
</tr>
<tr>
<td>PREFIX</td>
<td>(multicast</td>
<td>unicast)</td>
</tr>
<tr>
<td>multicast</td>
<td>Specifies a IPv4 multicast address family.</td>
<td>-</td>
</tr>
<tr>
<td>unicast</td>
<td>Specifies a IPv4 unicast address family. This is the default option.</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

N/A

**Usage**

N/A

**Examples**

Switch# show ip bgp community 10:23 exact-match
Switch# show ip bgp ipv4 multicast community 10:23 exact-match

**Related Commands**

N/A

**6.7.77 show ip bgp community-info**

**Command Purpose**

Use this command to list all BGP community information.
Command Syntax
show ip bgp community-info

Command Mode
Privileged EXEC

Default
N/A

Usage
N/A

Examples
Switch# show ip bgp community-info

Related Commands
N/A

6.7.78  show ip bgp community-list

Command Purpose
Use this command to display routes that match the community-list.

Command Syntax
show ip bgp community-list LISTNAME ( exact-match | )
show ip bgp ipv4 PREFIX community-list LISTNAME ( exact-match | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISTNAME</td>
<td>Specifies the community list name.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>exact-match</td>
<td>Displays only routes that have exactly the same specified communities.</td>
<td>-</td>
</tr>
<tr>
<td>ipv4</td>
<td>Specifies the address family. The type of address family determines the routing table that is displayed.</td>
<td>-</td>
</tr>
<tr>
<td>PREFIX</td>
<td>(multicast</td>
<td>unicast)</td>
</tr>
<tr>
<td>unicast</td>
<td>Specifies a IPv4 unicast address family. This is the default option.</td>
<td>-</td>
</tr>
<tr>
<td>multicast</td>
<td>Specifies a IPv4 multicast address family.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
N/A
Usage

N/A

Examples

Switch# show ip bgp community-list mylist exact-match
Switch# show ip bgp ipv4 unicast community-list mylist

Related Commands

N/A

6.7.79 show ip bgp dampening

Command Purpose

Use this command to display detailed information about dampening.

Command Syntax

```
show ip bgp dampening ( dampened-paths | flap-statistics | parameters )
show ip bgp ipv4 PREFIX dampening ( dampened-paths | flap-statistics | parameters )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dampened-paths</td>
<td>Display paths suppressed due to dampening.</td>
<td>-</td>
</tr>
<tr>
<td>flap-statistics</td>
<td>Display flap statistics of routes.</td>
<td>-</td>
</tr>
<tr>
<td>parameters</td>
<td>Display details of configured dampening parameters.</td>
<td>-</td>
</tr>
<tr>
<td>ipv4</td>
<td>Specifies the address family. The type of address family determines the routing table that is displayed.</td>
<td>-</td>
</tr>
<tr>
<td>PREFIX</td>
<td>(multicast</td>
<td>unicast)</td>
</tr>
<tr>
<td>unicast</td>
<td>Specifies an IPv4 unicast address family. This is the default option.</td>
<td>-</td>
</tr>
<tr>
<td>multicast</td>
<td>Specifies an IPv4 multicast address family.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

N/A
Usage
N/A

Examples
Enable bgp dampening to maintain dampened-path information in memory. The following is a sample output displaying all the dampening parameters:

```
Switch# show ip bgp dampening parameters
```

Related Commands
N/A

6.7.80 show ip bgp filter-list

Command Purpose
Use this command to display routes conforming to the filter-list.

Command Syntax
```
show ip bgp filter-list LISTNAME
show ip bgp ipv4 PREFIX filter-list LISTNAME
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISTNAME</td>
<td>Specifies the regular-expression access list name.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>ipv4</td>
<td>Specifies the address family. The type of address family determines the routing table that is displayed.</td>
<td>-</td>
</tr>
<tr>
<td>PREFIX</td>
<td>(multicast</td>
<td>unicast)</td>
</tr>
<tr>
<td>unicast</td>
<td>Specifies an IPv4 unicast address family. This is the default option.</td>
<td>-</td>
</tr>
<tr>
<td>multicast</td>
<td>Specifies an IPv4 multicast address family.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
N/A

Usage
N/A
Examples

Switch# show ip bgp filter-list mylist
Switch# show ip bgp ipv4 unicast filter-list Switch

Related Commands

N/A

6.7.81 show ip bgp inconsistent-as

Command Purpose

Use this command to display routes with inconsistent AS Paths.

Command Syntax

show ip bgp inconsistent-as
show ip bgp ipv4 PREFIX inconsistent-as

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>Specifies the address family. The type of address family determines the</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>routing table that is displayed.</td>
<td></td>
</tr>
<tr>
<td>PREFIX</td>
<td>(multicast</td>
<td>unicast)</td>
</tr>
<tr>
<td>unicast</td>
<td>Specifies an IPv4 unicast address family. This is the default option.</td>
<td>-</td>
</tr>
<tr>
<td>multicast</td>
<td>Specifies an IPv4 multicast address family.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

Switch# show ip bgp inconsistent-as
Switch# show ip bgp ipv4 unicast inconsistent-as
Related Commands

N/A

6.7.82 show ip bgp neighbors

Command Purpose

Use this command to display detailed information on TCP and BGP neighbor connections.

Command Syntax

show ip bgp neighbors (IPADDRESS (advertised-routes | RECEIVED | received-routes | routes | ))
show ip bgp ipv4 PREFIX neighbors (IPADDRESS (advertised-routes | received | received-routes | routes | ))

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPADDRESS</td>
<td>Specifies an IPv4 address.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
<tr>
<td>advertised-routes</td>
<td>Displays the routes advertised to a BGP neighbor.</td>
<td>-</td>
</tr>
<tr>
<td>received</td>
<td>received prefix-filter Displays all received routes, both accepted and rejected.</td>
<td>-</td>
</tr>
<tr>
<td>prefix-filter</td>
<td>Displays the prefix-list filter.</td>
<td>-</td>
</tr>
<tr>
<td>received-routes</td>
<td>Displays the received routes from neighbor.</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>To display all the received routes from the neighbor, configure the BGP soft reconfigure first. routes Displays all accepted routes learned from neighbors.</td>
<td>-</td>
</tr>
<tr>
<td>routes</td>
<td>Display routes learned from neighbor</td>
<td>-</td>
</tr>
<tr>
<td>PREFIX</td>
<td>(multicast</td>
<td>unicast)</td>
</tr>
<tr>
<td>unicast</td>
<td>Specifies a IPv4 unicast address family. This is the default option.</td>
<td>-</td>
</tr>
<tr>
<td>multicast</td>
<td>Specifies a IPv4 multicast address family.</td>
<td>-</td>
</tr>
<tr>
<td>ipv4</td>
<td>Specifies the address family. The type of address family determines the routing table that is displayed.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A
Examples

This is a sample output from the `show ip bgp neighbors` command displaying information about the specified neighbor:

```
Switch# show ip bgp neighbors
```

Related Commands

N/A

6.7.83  `show ip bgp paths`

Command Purpose

Use this command to display BGP path information.

Command Syntax

```
show ip bgp paths
show ip bgp ipv4 PREFIX paths
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>Specifies the address family. The type of address family determines the routing table that is displayed.</td>
<td>-</td>
</tr>
<tr>
<td>PREFIX</td>
<td>(multicast</td>
<td>unicast)</td>
</tr>
<tr>
<td>unicast</td>
<td>Specifies a IPv4 unicast address family. This is the default option.</td>
<td>-</td>
</tr>
<tr>
<td>multicast</td>
<td>Specifies a IPv4 multicast address family.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# show ip bgp paths
```
Related Commands

N/A

6.7.84 show ip bgp prefix-list

Command Purpose

Use this command to display routes matching the prefix-list.

Command Syntax

show ip bgp prefix-list LIST
show ip bgp ipv4 PREFIX prefix-list LIST

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIST</td>
<td>Specifies the name of the IP prefix list.</td>
<td>Up to 40 characters</td>
</tr>
<tr>
<td>ipv4</td>
<td>Specifies the address family. The type of address family determines the routing table that is displayed.</td>
<td>-</td>
</tr>
<tr>
<td>PREFIX</td>
<td>(multicast</td>
<td>unicast)</td>
</tr>
<tr>
<td>multicast</td>
<td>Specifies a IPv4 multicast address family. This is the default option.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

Switch# show ip bgp prefix-list mylist

Related Commands

N/A
6.7.85  show ip bgp quote-regexp

Command Purpose

Use this command to display routes matching the AS path regular expression in quotes.

Command Syntax

show ip bgp quote-regexp LINE
show ip bgp ipv4 PREFIX quote-regexp LINE

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LINE</td>
<td>Specifies a regular-expression to match the BGP AS paths</td>
<td>A regular-expression in quote</td>
</tr>
<tr>
<td>ipv4</td>
<td>Specifies the address family. The type of address family determines the routing table that is displayed.</td>
<td>-</td>
</tr>
<tr>
<td>PREFIX</td>
<td>(multicast</td>
<td>unicast)</td>
</tr>
<tr>
<td>unicast</td>
<td>Specifies an IPv4 unicast address family. This is the default option.</td>
<td>-</td>
</tr>
<tr>
<td>multicast</td>
<td>Specifies an IPv4 multicast address family.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

Switch# show ip bgp quote-regexp "Switch"

Related Commands

N/A
6.7.86 show ip bgp regexp

Command Purpose

Use this command to display routes matching the AS path regular expression.

Command Syntax

show ip bgp regexp LINE
show ip bgp ipv4 PREFIX regexp LINE

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>regexp</td>
<td>Displays routes matching the AS path regular expression.</td>
<td>-</td>
</tr>
<tr>
<td>LINE</td>
<td>Specifies a regular expression to match the BGP AS paths.</td>
<td>A regular-expression</td>
</tr>
<tr>
<td>ipv4</td>
<td>Specifies the address family. The type of address family determines the routing table that is displayed.</td>
<td>-</td>
</tr>
<tr>
<td>PREFIX</td>
<td>(multicast</td>
<td>unicast)</td>
</tr>
<tr>
<td>unicast</td>
<td>Specifies a IPv4 unicast address family. This is the default option.</td>
<td>-</td>
</tr>
<tr>
<td>multicast</td>
<td>Specifies a IPv4 multicast address family.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

Switch# show ip bgp regexp myexpression

Related Commands

N/A
6.7.87  show ip bgp scan

Command Purpose
Use this command to display BGP scan status.

Command Syntax
show ip bgp scan

Command Mode
Privileged EXEC

Default
N/A

Usage
N/A

Examples
Switch# show ip bgp scan

Related Commands
N/A

6.7.88  show ip bgp summary

Command Purpose
Use this command to display a summary of BGP neighbor status.

Command Syntax
show ip bgp summary
show ip bgp ipv4 PREFIX summary

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>Specifies the address family. The type of address family determines the routing table that is displayed.</td>
<td>-</td>
</tr>
<tr>
<td>PREFIX</td>
<td>(multicast</td>
<td>unicast)</td>
</tr>
<tr>
<td>unicast</td>
<td>Specifies a IPv4 unicast address family. This is the default option.</td>
<td>-</td>
</tr>
<tr>
<td>multicast</td>
<td>Specifies a IPv4 multicast address family.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC
Default

N/A

Usage

N/A

Examples

This is a sample output from the show ip bgp summary command displaying a summary of BGP neighbor status:

```
Switch# show ip bgp summary
```

Related Commands

N/A

6.7.89  show ip bgp vpnv4 all

Command Purpose

Use this command to display VPNv4 NLRI specific information.

Command Syntax

```
show ip bgp vpnv4 all TYPE
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays information about all VPNv4 NLRIs</td>
<td>-</td>
</tr>
<tr>
<td>TYPE</td>
<td>(A.B.C.D</td>
<td>neighbors</td>
</tr>
<tr>
<td>neighbors</td>
<td>Displays information about BGP neighbors.</td>
<td>-</td>
</tr>
<tr>
<td>summary</td>
<td>Displays summary of the BGP neighbor status.</td>
<td>-</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Network for which information will be displayed in the BGP routing table.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

N/A
Usage

N/A

Examples

This is a sample output from the `show ip bgp vpnv4 all` command displaying VPNv4 specific information:

```
Switch# show ip bgp vpnv4 all
```

Related Commands

N/A

6.7.90 `show ip bgp vpnv4 rd`

Command Purpose

Use this command to display VPNv4 NLRI specific information.

Command Syntax

```
show ip bgp vpnv4 rd WORD TYPE
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>rd</td>
<td>Display information for a route distinguisher</td>
<td>-</td>
</tr>
<tr>
<td>WORD</td>
<td>VPN Route Distinguisher</td>
<td>Up to 15 characters</td>
</tr>
<tr>
<td>TYPE</td>
<td>(A.B.C.D</td>
<td>neighbors</td>
</tr>
<tr>
<td>neighbors</td>
<td>Displays information about BGP neighbors.</td>
<td>-</td>
</tr>
<tr>
<td>summary</td>
<td>Displays summary of the BGP neighbor status.</td>
<td>-</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Network for which information will be displayed in the BGP routing table.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A
**Examples**

This is a sample output from the show ip bgp vpnv4 rd command displaying VPNv4 specific information:

```
Switch# show ip bgp vpnv4 rd 123
```

**Related Commands**

N/A

**6.7.91 show ip bgp vpnv4 vrf**

**Command Purpose**

Use this command to display VPNv4 NLRI specific information.

**Command Syntax**

```
show ip bgp vpnv4 vrf WORD TYPE
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf</td>
<td>VPN Routing/Forwarding instance</td>
<td>-</td>
</tr>
<tr>
<td>WORD</td>
<td>VPN Routing/Forwarding instance name</td>
<td>Up to 15 characters</td>
</tr>
<tr>
<td>TYPE</td>
<td>(A.B.C.D</td>
<td>neighbors</td>
</tr>
<tr>
<td>neighbors</td>
<td>Displays information about BGP neighbors.</td>
<td>-</td>
</tr>
<tr>
<td>summary</td>
<td>Displays summary of the BGP neighbor status.</td>
<td>-</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Network for which information will be displayed in the BGP routing table.</td>
<td>IPv4 Address in A.B.C.D format</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

N/A

**Usage**

N/A
**Examples**

This is a sample output from the `show ip bgp vpnv4 rd` command displaying VPNv4 specific information:

```
Switch# show ip bgp vpnv4 vrf 123
```

**Related Commands**

N/A

**6.7.92 timers**

**Command Purpose**

Use this command sets the BGP keepalive timer and holdtime timer values.

Use the no parameter with this command to reset timers to default value.

**Command Syntax**

```
timers bgp KEEPALIVE HOLDTIME
no timers bgp
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEEPALIVE</td>
<td>&lt;0-65535&gt; The frequency with which the keepalive messages are sent to the neighbors. The default value is 60 seconds.</td>
<td>0-65535</td>
</tr>
<tr>
<td>HOLDTIME</td>
<td>The interval after which the neighbor is considered dead if keepalive messages are not received. The default holdtime value is 180 seconds.</td>
<td>3-65535</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration

**Default**

N/A

**Usage**

This command is used globally to set or unset the keepalive and holdtime values for all the neighbors.

**Examples**

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# timers bgp 40 120
```
Related Commands

N/A

6.8 ISIS Commands

6.8.1 accept-lifetime

Command Purpose

Use this command to specify the time period during which the authentication on a key chain is received as valid.
Use the no parameter with this command to negate this command.

Command Syntax

accept-lifetime HH:MM:SS MONTH YEAR HH1:MM1:SS1 DAY1 MONTH1 YEAR1
accept-lifetime HH:MM:SS MONTH DAY YEAR infinite
accept-lifetime HH:MM:SS MONTH DAY YEAR duration <1-2147483646>
no accept-lifetime

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HH:MM:SS</td>
<td>Specify the end time of accept-lifetime in hours, minutes and seconds.</td>
<td>0:23:0-59:0-59</td>
</tr>
<tr>
<td>DAY</td>
<td>Specify the day of the month to end.</td>
<td>1-31</td>
</tr>
<tr>
<td>MONTH</td>
<td>Specify the month of the year to end as the first three letters of the month, for example, december.</td>
<td>january, february, march, april, may, june, july, august, september, october, november, december</td>
</tr>
<tr>
<td>YEAR</td>
<td>Specify the year to end.</td>
<td>1993-2035</td>
</tr>
<tr>
<td>HH1:MM1:SS1</td>
<td>Specify the year to end.</td>
<td>0-23:0-59:0-59</td>
</tr>
<tr>
<td>DAY1</td>
<td></td>
<td>1-31</td>
</tr>
<tr>
<td>MONTH1</td>
<td>january, february, march, april, may, june, july, august, september, october, november, december</td>
<td></td>
</tr>
<tr>
<td>YEAR1</td>
<td></td>
<td>1993-2035</td>
</tr>
<tr>
<td>&lt;1-2147483646&gt;</td>
<td>Specify the actual end time duration of a key in seconds.</td>
<td>1-2147483646</td>
</tr>
</tbody>
</table>

Command Mode

Key Chain Configuration

Default

None
Usage

None

Examples

The following example shows how to specify the time period during which the authentication on a key chain is received as valid:

Switch# configure terminal
Switch(config)# key chain mychain
Switch(config-keychain)# key 1
Switch(config-keychain-key)# accept-lifetime 03:03:01 Dec 3 2004 04:04:02 Oct 6 2006

Related Commands

None

6.8.2 address-family ipv6

Command Purpose

Use this command to enter ‘address-family ipv6’ mode, where users can configure IPv6 routing specific configuration. Use the no parameter with this command to remove all configuration under ‘address-family ipv6’.

Command Syntax

address-family ipv6 ( unicast | | )
no address-family ipv6 ( unicast | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>unicast</td>
<td>Specify unicast routing for IPv6.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

None

Usage

None
Examples

The following example shows how to enter ‘address-family ipv6’ mode:

Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# address-family ipv6 unicast
Switch(config-router-af)#

Related Commands

None

6.8.3 adjacency-check

Command Purpose

Use this command to configure the policy of adjacency based on the protocol related TLVs in the Hello packet. Check adjacency with protocol related TLVs including Protocols Supported TLV or IP Interface Address TLV by default. The command with no parameter disables this check.

Use the no parameter with this command to disable the adjacency check.

Command Syntax

adjacency-check
no adjacency-check

Command Mode

Router Configuration
Address Family Configuration

Default

Enabled

Usage

None

Examples

The following example shows how to enable adjacency check:

Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router-af)# adjacency-check
Related Commands

None

6.8.4 area-password

Command Purpose

Use this command to set the authentication password for the Level-1 area and to set authentication on Level-1 SNP PDUs. This command enables authentication when receiving and sending LSP and SNP PDU in Level-1 areas. Area password must be the same for all the routers in the same area.

Use the no parameter with this command to clear the area password.

Command Syntax

area-password PASSWORD
area-password WORD authenticate snp (send-only | validate)
no area-password

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PASSWORD</td>
<td>Specify the password string.</td>
<td>Up to 254 characters</td>
</tr>
<tr>
<td>authenticate</td>
<td>Specify to insert the password into Level-1 SNP PDUs.</td>
<td>-</td>
</tr>
<tr>
<td>snp</td>
<td>Specify the sequence number PDU (SNP).</td>
<td>-</td>
</tr>
<tr>
<td>send-only</td>
<td>Specify to only insert the password into the Level-1 SNP PDUs, but not check the password in SNP PDUs that it receives. Use this keyword during a software upgrade to ease the transition.</td>
<td>-</td>
</tr>
<tr>
<td>validate</td>
<td>Specify to insert the password into the Level-1 SNP PDUs and check the password in SNPs that it receives.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

Not configured

Usage

None
Examples

The following example shows how to set the authentication password for the Level-1 area:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# area-password code1234
```

Switch(config-router)# no area-password

Related Commands

None

6.8.5 authentication key-chain

Command Purpose

Use this command to set the key chain to be used for authentication at the instance level. Authentication mode must be set to md5 to configure the key chain. If no key chain is configured with the key-chain command, no key-chain authentication is performed. Only one authentication key-chain is applied to an interface at a time. That is, issuing a second isis authentication key-chain command overrides the first isis authentication key-chain command. Authentication can be specified for an individual interface using the isis authentication key-chain command.

Use the no parameter with this command to unset the key chain used for authentication.

Command Syntax

```
authentication key-chain WORD ( level-1 | level-2 | )
no authentication key-chain PASSWORD ( level-1 | level-2 | )
no authentication key-chain ( level-1 | level-2 | )
```

Parameter | Parameter Description | Parameter Value |
--- | --- | --- |
WORD | Specify the chain name (valid authentication keys). | A String of key chain name |
level-1 | Specify an authentication key-chain for level-1 PDUs. | - |
level-2 | Specify an authentication key-chain for level-2 PDUs. | - |

Command Mode

Router Configuration

Default

Disabled
Usage

If neither the level-1 nor the level-2 keyword is configured, it applies to both levels.

Examples

The following example shows how to set the key chain to be used for authentication at the level-1:

Switch# configure terminal
Switch(config)# router isis 1
Switch(config-router)# authentication key-chain code1234 level-1

Related Commands

None

6.8.6 authentication mode md5

Command Purpose

Use this command to set the MD5 authentication mode at the instance level. If clear-text authentication was configured using the area-password or domain-password commands, the authentication mode command overrides both of those commands (based on the level at which MD5 is configured). If the authentication mode command was used first, and subsequently an attempt is made to use the area-password or domain-password commands, the attempt fails. To configure clear-text authentication using the area-password or domain-password commands, first use the no authentication mode command. The type of authentication and the level to which it applies can be specified for a single interface, rather than per instance, using the isis authentication mode command. Use the no parameter with this command to unset the MD5 authentication mode.

Command Syntax

authentication mode (md5 | text) (level-1 | level-2)
no authentication mode (md5 | text) (level-1 | level-2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>md5</td>
<td>Keyed message digest</td>
<td>-</td>
</tr>
<tr>
<td>text</td>
<td>Text mode</td>
<td>-</td>
</tr>
<tr>
<td>level-1</td>
<td>Specify an authentication key-chain for level-1 PDUs.</td>
<td>-</td>
</tr>
<tr>
<td>level-2</td>
<td>Specify an authentication key-chain for level-2 PDUs.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration
Default

Disabled

Usage

If neither the level-1 nor the level-2 keyword is configured, it applies to both levels.

Examples

The following example shows how to set the MD5 authentication mode at the level-1:

Switch# configure terminal
Switch(config)# router isis 1
Switch(config-router)# authentication mode md5 level-1
Switch(config-router)# no authentication mode md5 level-1

Related Commands

None

6.8.7 authentication send-only

Command Purpose

Use this command to set the send-only option at the instance level.
Use this command before configuring the authentication mode and authentication key-chain, so that the implementation of authentication goes smoothly.
After all routers that must communicate are configured with this command, enable the authentication mode and key chain on each router.
Then, specify the no authentication send-only command to disable the send-only feature.
If neither the level-1 nor level-2 keyword is configured, the send-only feature applies to both levels. The send-only option applies to both levels if no level is specified.
Use the no parameter with this command to unset the send-only option.

Command Syntax

authentication send-only (level-1 | level-2 |) 
no authentication send-only (level-1 | level-2 |)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-1</td>
<td>Specify an authentication key-chain for level-1 PDUs.</td>
<td>-</td>
</tr>
<tr>
<td>level-2</td>
<td>Specify an authentication key-chain for level-2 PDUs.</td>
<td>-</td>
</tr>
</tbody>
</table>
Command Mode

Router Configuration

Default

Disabled

Usage

If neither the level-1 nor the level-2 keysword is configured, it applies to both levels.

Examples

The following example shows how to set the send-only option at the level-1:

```
Switch# configure terminal
Switch(config)# router isis 1
Switch(config-router)# authentication send-only level-1
Switch(config-router)# no authentication send-only level-1
```

Related Commands

None

6.8.8 bfd all/interfaces

Command Purpose

Use this command to enable the Bidirectional Forwarding Detection (BFD) feature on the interfaces enabled with this ISIS instance. This command sets BFD fall-over check for all the neighbors under specified process. To disable BFD checking on particular interface use `isis bfd disable` command at interface mode. Use the no parameter with this command to disable BFD functionality for an instance.

Command Syntax

```
bfd all-interfaces
no bfd all-interfaces
```

Command Mode

Router Configuration
Default
Disabled

Usage
None

Examples

The following example shows how to enable the BFD feature on the interfaces enabled with this ISIS instance:

```
Switch# configure terminal
Switch(config)# router isis
Switch(config-router)# bfd all-interfaces
```

Related Commands

None

6.8.9 clear clns neighbors

Command Purpose
Use this command to clear CLNS neighbor adjacencies.

Command Syntax
clear clns neighbors

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples

The example shows how to clear CLNS neighbor adjacencies:

```
Switch# clear clns neighbors
```

Related Commands

None
6.8.10 clear clns is-neighbors

Command Purpose

Use this command to clear IS neighbor adjacencies.

Command Syntax

clear clns is-neighbors System-ID

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>System-ID</td>
<td>Neighbor system ID in XXXXXXXXXX.XXXX format.</td>
<td>hexadecimal</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The example shows how to clear IS neighbor adjacencies:

Switch# clear clns is-neighbors 1234.789A.BCDF

Related Commands

None

6.8.11 clear ip isis route

Command Purpose

Use this command to clear IPv4 routes.

Command Syntax

clear ip isis ( INSTANCE | ) route ( redistribution | all )
### Command Mode

Privileged EXEC

### Default

None

### Usage

None

### Examples

The example shows how to clear ISIS IPv4 routes:

```
Switch# clear ip isis route all
```

### Related Commands

None

#### 6.8.12 clear isis counter

### Command Purpose

Use this command to clear system-wide IS-IS counters

### Command Syntax

```
clear isis counter
```

### Command Mode

Privileged EXEC

### Default

None
Usage

None

Examples

The example shows how to clear system-wide IS-IS counters:

Switch# clear isis counter

Related Commands

None

6.8.13 clear isis interface counter

Command Purpose

Use this command to clear interface counters.

Command Syntax

```
clear isis interface counter (IFNAME |)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name.</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

If you do not specify a parameter, then counters for all interfaces are cleared.

Examples

The example shows how to clear clear interface counters:

Switch# clear isis interface counter
Related Commands

None

6.8.14 clear isis process

Command Purpose

Use this command to restart ISIS processes.

Command Syntax

clear isis (INSTANCE |) process

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE</td>
<td>Routing area tag.</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

If you do not specify a parameter, then all ISIS processes are restarted.

Examples

The example shows how to restart ISIS processes:

Switch# clear isis process

Related Commands

None

6.8.15 debug isis

Command Purpose

Use this command to turn on debugging for specified criteria. Debug commands enable to show some debugging information about specified criteria into file or terminal.
Use the no parameter to turn off debugging for specified criteria.

**Command Syntax**

```plaintext
debug isis (all | )
debug isis (authentication | bfd | checksum | events | hello ( interface IFNAME | System-ID | ) | ifsm | local-updates | lsp | nfsm | nsm | pdu | protocol-errors | spf )
no debug isis (all | )
no debug all
no debug all isis
undebug all
undebug all isis
no debug isis (authentication | bfd | checksum | events | hello ( interface IFNAME | System-ID | ) | ifsm | local-updates | lsp | nfsm | nsm | pdu | protocol-errors | spf )
undebug isis (authentication | bfd | checksum | events | hello ( interface IFNAME | System-ID | ) | ifsm | local-updates | lsp | nfsm | nsm | pdu | protocol-errors | spf )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enables all debugging.</td>
<td>-</td>
</tr>
<tr>
<td>authentication</td>
<td>Debugging for authentication.</td>
<td>-</td>
</tr>
<tr>
<td>checksum</td>
<td>Debugging for checksums.</td>
<td>-</td>
</tr>
<tr>
<td>bfd</td>
<td>Debugging for bidirectional forwarding detection.</td>
<td>-</td>
</tr>
<tr>
<td>events</td>
<td>Debugging for internal events.</td>
<td>-</td>
</tr>
<tr>
<td>hello</td>
<td>Debugging for hello processing.</td>
<td>-</td>
</tr>
<tr>
<td>interface</td>
<td>Interface.</td>
<td>-</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Interface name.</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
<tr>
<td>System-ID</td>
<td>System identifier.</td>
<td>-</td>
</tr>
<tr>
<td>ifsm</td>
<td>Debugging for interface finite state machine.</td>
<td>-</td>
</tr>
<tr>
<td>local-updates</td>
<td>Debugging for local updates.</td>
<td>-</td>
</tr>
<tr>
<td>lsp</td>
<td>Debugging for label switched path.</td>
<td>-</td>
</tr>
<tr>
<td>nfsm</td>
<td>Debugging for neighbor finite state machine.</td>
<td>-</td>
</tr>
<tr>
<td>nsm</td>
<td>Debugging for NSM messages.</td>
<td>-</td>
</tr>
<tr>
<td>pdu</td>
<td>Debugging for protocol data unit.</td>
<td>-</td>
</tr>
<tr>
<td>protocol-errors</td>
<td>Debugging for protocol errors.</td>
<td>-</td>
</tr>
<tr>
<td>spf</td>
<td>Debugging for shortest path first route calculation.</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC
Default

Disabled

Usage

None

Examples

The example shows how to enable all isis debugging:

Switch# debug isis all

Related Commands

None

6.8.16 default-information originate

Command Purpose

Use this command to originate reachability information to Default destination into LSP. There is no default information in Level-2 domain by default, while Level-1 router calculates default to L1L2 route SPF calculation. This command enables to originate default route into Level-2 domain. Use the no parameter with this command to withdraw reachability information to default destination from LSP.

Command Syntax

default-information originate

no default-information originate

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>originate</td>
<td>Specify to distribute a default route</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration
Address Family Configuration

Default

Disabled
Usage

None

Examples

The following example shows how to originate reachability information to Default destination into LSP both ipv4 and ipv6:

Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# default-information originate
Switch(config-router)# address-family ipv6
Switch(config-router-af)# default-information originate

Related Commands

None

6.8.17 distance

Command Purpose

Use this command in router mode to set the administrative distance for all IPv4 routes.
Use the no parameter with this command to remove an administrative distance.

Command Syntax

distance DISTANCE ( System-ID ( ACL | ) ) |
no distance ( ( System-ID | System-ID ACL ) | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISTANCE</td>
<td>Distance range.</td>
<td>1-255</td>
</tr>
<tr>
<td>System-ID</td>
<td>Source ID in XXXX.XXXX.XXXX format.</td>
<td>hexadecimal</td>
</tr>
<tr>
<td>ACL</td>
<td>Access-list name.</td>
<td>Up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

None

Usage

None
Examples

The following example shows how to set the administrative distance for all ISIS IPv4 routes:

Switch# configure terminal
Switch(config)# router isis
Switch(config-router)# distance 40

Related Commands

None

6.8.18 domain-password

Command Purpose

Use this command to set the authentication password for the Level-2 domain, and optionally, the authentication password on Level-2 SNP PDUs. Configuring this command to enable authentication when receiving and sending LSP and SNP PDU in Level-2 domain. Domain password must be the same in Level-2 domain.

Use the no parameter with this command to clear the domain password.

Command Syntax

domain-password PASSWORD
domain-password PASSWORD authenticate snp ( send-only | validate )
no domain-password

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PASSWORD</td>
<td>The password string.</td>
<td>Up to 254 characters</td>
</tr>
<tr>
<td>authenticate</td>
<td>Inserts the password into Level-2 SNP PDUs.</td>
<td>-</td>
</tr>
<tr>
<td>snp</td>
<td>SNP PDUs.</td>
<td>-</td>
</tr>
<tr>
<td>send-only</td>
<td>Only inserts the password into the Level-2 SNP PDUs, but does not check the password in SNP PDUs that it receives. Use this keyword during a software upgrade to ease the transition.</td>
<td>-</td>
</tr>
<tr>
<td>validate</td>
<td>Inserts the password into the Level-2 SNP PDUs, and checks the password in SNP PDUs that it receives.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration
Default

By default, there is no domain password.

Usage

None

Examples

The following example shows how to set the authentication password for the Level-2 domain:

Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# domain-password mypasswd
Switch(config-router)# no domain-password

Related Commands

None

6.8.19 ignore-lsp-errors

Command Purpose

Use this command to ignore LSPs with checksum errors. By default, validates checksum for LSP whenever it receives LSPs and if the checksum has an error, the LSP will be dropped. Configuring this command to ignore the LSP checksum error and treat it as if checksum is passed.

Use the no parameter to turn off this function.

Command Syntax

ignore-lsp-errors
no ignore-lsp-errors

Command Mode

Router Configuration

Default

Disabled
Usage

None

Examples

The following example shows how to ignore LSPs with checksum errors:

Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# ignore-lsp-errors

Related Commands

None

6.8.20 ip route high-priority tag

Command Purpose

Use this command to set a high priority tag value.
Use the no parameter to turn off this function.

Command Syntax

ip route high-priority tag TAG
no ip route high-priority tag

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TAG</td>
<td>Tag value</td>
<td>1-4294967295</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

Disabled

Usage

None

Examples

The following example shows how to set a high priority tag value:

Switch# configure terminal
Switch(config)# router isis A
Switch(config-router)# ip route high-priority tag 500
Related Commands
None

6.8.21 ip router isis

Command Purpose

Use this command to enable IPv4 routing on the interface. This command is mandatory to configuration. Match the instance tag to one of existing instance’s tags, or a new instance with the tag name should be initiated, otherwise routing will not run on this interface. Configuring this command, the router sends Hello with IP address TLV on this interface, and IP reachability information TLV in the LSP will be updated.

Use the no parameter with this command to disable IPv4 routing on the interface. This action does not clear the database. To clear the database, unconfigure the routing instance.

Command Syntax

ip router isis (INSTANCE | )
no ip router isis (INSTANCE | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE</td>
<td>instance name.</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

Disabled

Usage

None

Examples

The following example shows how to enable ISIS IPv4 routing on the interface:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ip router isis bb

Related Commands
None
6.8.22  ipv6 router isis

Command Purpose

Use this command to enable IPv6 routing on the interface. This command is mandatory to IPv6 configuration. Match the instance tag to one of existing instance’s tags, or a new instance with the tag name should be initiated, otherwise routing will not run on this interface. Configuring this command, the router sends Hello with IPv6 address TLV on this interface, and IPv6 reachability information TLV in the LSP will be updated.

Use the no parameter with this command to disable IPv6 routing on the interface.

Command Syntax

ipv6 router isis (INSTANCE | )
no ipv6 router isis (INSTANCE | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE</td>
<td>instance name.</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

Disabled

Usage

None

Examples

The following example shows how to enable ISIS IPv6 routing on the interface:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 router isis bb

Related Commands

None
### 6.8.23 isis authentication key-chain

**Command Purpose**

Use this command to set the key chain to be used for authentication on the interface-related packets. Authentication mode must be set to md5 or text to configure the key chain. If no key chain is configured with the key-chain command, no key-chain authentication is performed. Only one authentication key-chain is applied to an interface at a time. That is, issuing a second isis authentication key-chain command overrides the first isis authentication key-chain command.

If neither the level-1 nor level-2 keyword is configured, the key chain applies to the level(s) on which the authentication mode is configured as md5. Authentication can be specified for an entire, instead of at the interface level, by using the authentication key-chain command.

Use the no parameter with this command to unset the key chain used for authentication on the interface-related packets.

**Command Syntax**

```plaintext
isis authentication key-chain KEY_NAME (level-1 | level-2 | )
no isis authentication key-chain ( level-1 | level-2 | )
no isis authentication key-chain KEY_NAME ( level-1 | level-2 | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEY_NAME</td>
<td>Chain name - valid authentication keys.</td>
<td>A String of key chain name</td>
</tr>
<tr>
<td>level-1</td>
<td>Specify an authentication key-chain for level-1 PDUs.</td>
<td>-</td>
</tr>
<tr>
<td>level-2</td>
<td>Specify an authentication key-chain for level-2 PDUs.</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

Disabled

**Usage**

The key chain applies to the level(s) on which authentication mode is configured as MD5 if no level is specified.

**Examples**

The following example shows how to set the key chain to be used for authentication on the interface-related packets:

```plaintext
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# isis authentication key-chain code1234 level-1
```

**Related Commands**

None
6.8.24  isis authentication mode md5

Command Purpose

Use this command to set the MDS authentication mode. If clear text authentication was configured using the isis password command, the isis authentication mode command overrides the isis password command. If the isis authentication mode command was used, then subsequently an attempt is made to use the isis password command, the attempt fails.

To configure clear text authentication using the isis password command, first use the no isis authentication mode command. The type of authentication and the level to which it applies can be specified for the entire instance, rather than per interface, using the authentication mode command.

Use the no parameter with this command to unset the MDS authentication mode.

Command Syntax

isis authentication mode (md5 | text) (level-1 | level-2 )
no isis authentication mode (md5 | text) (level-1 | level-2 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>md5</td>
<td>Keyed message digest</td>
<td>-</td>
</tr>
<tr>
<td>text</td>
<td>Text mode</td>
<td>-</td>
</tr>
<tr>
<td>level-1</td>
<td>Specify an authentication key-chain for level-1 PDUs.</td>
<td>-</td>
</tr>
<tr>
<td>level-2</td>
<td>Specify an authentication key-chain for level-2 PDUs.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
Disabled

Usage
The send-only option applies to both levels if no level is specified.

Examples
The following example shows how to set the MDS authentication mode:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# isis authentication mode md5

Related Commands
None
6.8.25 **isis authentication send-only**

**Command Purpose**

Use this command to set the send-only option to the interface-related packets.

Use this command before configuring the ISIS authentication mode and ISIS authentication key-chain, so that the implementation of authentication goes smoothly. That is, the routers will have more time for the keys to be configured on each router if authentication is inserted only on the packets being sent, not checked on packets being received.

After all routers that must communicate are configured with this command, enable the authentication mode and key chain on each router.

Use the no parameter with this command to unset the send-only option to the interface-related packets.

**Command Syntax**

```
isis authentication send-only (level-1 | level-2 )
no isis authentication send-only (level-1 | level-2 )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-1</td>
<td>Specify an authentication key-chain for level-1 PDUs.</td>
<td>-</td>
</tr>
<tr>
<td>level-2</td>
<td>Specify an authentication key-chain for level-2 PDUs.</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

Disabled

**Usage**

The send-only option applies to both levels if no level is specified.

**Examples**

The following example shows how to set the send-only option to the interface-related packets:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# isis authentication send-only
```

**Related Commands**

None
6.8.26 isis bfd

Command Purpose

Use this command to enable/disable the BFD check on interface. The `isis bfd` command allows a user to enable BFD on an interface. The `isis bfd disable` command disables BFD checking on an interface. However, the `no isis bfd` and `no isis bfd disable` commands both remove the enable/disable configuration, but do not disable/enable BFD. The `bfd all-interfaces` command enables BFD on all interfaces attached to an instance then configuring. This command disables BFD configuration on a particular interface.

Command Syntax

```
isis bfd (disable |)
no isis bfd (disable |)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Specify to disable BFD.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

Disabled

Usage

None

Examples

The following example shows how to disable bfd on ISIS interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# isis bfd disable
```

Related Commands

None
6.8.27 **isis circuit-type**

**Command Purpose**

Use this command to set the circuit type for the interface.

If level-1 or level-2-only is specified in this command, sends only the specified level of PDUs.

Use the no parameter to reset circuit type to the default.

**Command Syntax**

```plaintext
isis circuit-type (level-1 | level-1-2 | level-2-only)

no isis circuit-type
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-1</td>
<td>Specify that only Level-1 adjacencies are formed.</td>
<td>-</td>
</tr>
<tr>
<td>level-1-2</td>
<td>Specify that Level-1-2 adjacencies are formed.</td>
<td>-</td>
</tr>
<tr>
<td>level-2-only</td>
<td>Specify that only Level-2 adjacencies are formed.</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

Enabled level-1 and level-2.

**Usage**

None

**Examples**

The following example shows how to set the circuit type for the interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# isis circuit-type level-2-only
```

**Related Commands**

None
6.8.28 isis csnp-interval

Command Purpose

Use this command to set CSNP (Complete sequence number PDU) interval in seconds. Configuring this command changes the interval between two consecutive CSNP transmission. By default, CSNP is sent every 10 seconds only by LAN DIS. This parameter is only valid on broadcast interface, since periodic CSNP is only sent on broadcast interface, while CSNP on Point-to-Point interface is sent only when adjacency is initiated. Use the no parameter with this command to reset CSNP interval to the default value.

Command Syntax

```bash
isis csnp-interval INTERVAL (level-1 | level-2 )
no isis csnp-interval (level-1 | level-2 )
no isis csnp-interval <1-65535> (level-1 | level-2 )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>Specify the CSNP interval in seconds.</td>
<td>1-65535</td>
</tr>
<tr>
<td>level-1</td>
<td>Specify Level-1 CSNP.</td>
<td>-</td>
</tr>
<tr>
<td>level-2</td>
<td>Specify Level-2 CSNP.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

10 seconds level-1 and level-2.

Usage

None

Examples

The following example shows how to set CSNP (Complete sequence number PDU) interval.:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# isis csnp-interval 20
```

Related Commands

None
6.8.29 isis hello

Command Purpose

Use this command to configure the padding of the Hello packet. Pads the Hello packet by default to notify neighbors of the supported MTU size.
Use the no parameter with this command to disable the padding.

Command Syntax

isis hello padding
no isis hello padding

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>padding</td>
<td>Specify pad hello packets</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

By default, pads the Hello packet.

Usage

None

Examples

The following example shows how to configure the padding of the Hello packet:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# isis hello padding

Related Commands

None

6.8.30 isis hello-interval

Command Purpose

Use this command to set the Hello interval in seconds. The Hello-interval is set with the hello-multiplier (see isis hello-multiplier command).
Configuring this command changes the time interval between two consecutive Hello transmissions. If a device receives its own LSP with a maximum sequence number, then it suspends for the hold interval. DIS sends Hello transmissions at three times the rate than non-DIS. If is elected as DIS on this interface, sends Hello every 3.3 seconds.

If minimal keywords is specified, Holding timer in Hello PDU is set to 1 second and Hello interval is calculated by dividing by the hello-multiplier. For example, if the hello-multiplier is configured as 4 and hello-interval minimal is the command used, an Hello PDU is sent every 250 milliseconds.

Use the no parameter to set the Hello interval to the default.

**Command Syntax**

```plaintext
isis hello-interval INTERVAL (level-1 | level-2 |)
isis hello-interval minimal (level-1 | level-2 |)
no isis hello-interval (level-1 | level-2 |)
no isis hello-interval <1-65535> (level-1 | level-2 |)
no isis hello-interval minimal (level-1 | level-2 |)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>Specify the hello interval in</td>
<td>1-65535</td>
</tr>
<tr>
<td>minimal</td>
<td>Specify the holding-time as</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>1 second.</td>
<td></td>
</tr>
<tr>
<td>level-1</td>
<td>Specify Level-1 CSNP.</td>
<td>-</td>
</tr>
<tr>
<td>level-2</td>
<td>Specify Level-2 CSNP.</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

By default, uses 10 seconds for the interval and the interval is applied to both level-1 and level-2.

**Usage**

If neither the level-1 nor the level-2 keywords is configured, it applies to both levels.

**Examples**

The following example shows how to set the Hello interval:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# isis hello-interval 5 level-1
```

**Related Commands**

`isis hello-multiplier`
6.8.31  **isis hello-multiplier**

**Command Purpose**

Use this command to set multiplier for Hello holding time.
Changes Holding Timer in Hello PDU. Holding timer is calculated by “Hello-Interval” multiplied by this value. If minimal keyword is specified with the Hello-Interval, the holding timer is set to 1 second and the hello-interval is calculated by dividing 1 by this value.
Use the no parameter with this command to set multiplier to the default.

**Command Syntax**

```bash
isis hello-MULTIPLIER <2-100> (level-1 | level-2 )
nosis hello-multiplier ( level-1 | level-2 )
nosis hello-multiplier <2-100> ( level-1 | level-2 )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MULTIPLIER</td>
<td>Specify a hello multiplier value.</td>
<td>2-100</td>
</tr>
<tr>
<td>level-1</td>
<td>Specify Level-1 hello.</td>
<td>-</td>
</tr>
<tr>
<td>level-2</td>
<td>Specify Level-2 hello.</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

By default, uses 3 seconds for the multiplier value and the multiplier is applied to both level-1 and level-2.

**Usage**

If neither the level-1 nor the level-2 keyword is configured, it applies to both levels.

**Examples**

The following example shows how to set multiplier for Hello holding time:

```bash
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# isis hello-multiplier 4
```

**Related Commands**

None
6.8.32 isis lsp-interval

Command Purpose

Use this command to set the Link State Packet (LSP) transmission interval. Configuring this command changes the minimum interval between two consecutive LSP transmission. When flooding or some other event triggers LSP to transmit, the LSP is put on the interface queue and scheduled to transmit according to this interval. Two consecutive LSP transmissions are scheduled to have at least this interval. Use the no parameter with this command to set LSP transmission interval to the default.

Command Syntax

isis lsp-interval INTERVAL
no isis lsp-interval

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>Specify an LSP transmission interval in milliseconds.</td>
<td>1-4294967295</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

By default, 33 milliseconds for the interval.

Usage

None

Examples

The following example shows how to set the Link State Packet (LSP) transmission interval:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# isis lsp-interval 100
```

Related Commands

None
6.8.33 isis mesh-group

Command Purpose

Use this command to set Mesh Group ID on the current interface.
Use the no parameter to unset mesh group on the current interface.

Command Syntax

isis mesh-group MESH_GROUP
isis mesh-group blocked
no isis mesh-group

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MESH_GROUP</td>
<td>Specify a mesh group number</td>
<td>1-4294967295</td>
</tr>
<tr>
<td>blocked</td>
<td>Specify to block LSPs on the current interface. If an interface is configured as &quot;mesh group blocked,&quot; the standard LSP database synchronization process is applied if the interface receives CSNP or PSNP.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

By default, mesh groups are not enabled on this interface.

Usage

None

Examples

The following example shows how to set Mesh Group ID on the current interface:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# isis mesh-group 20

Related Commands

None
6.8.34  **isis metric**

**Command Purpose**

Use this command to set default metric for the interface. The interface default metric is put into IP reachability information TLVs, IS reachability information TLVs and IPv6 reachability TLVs in LSPs. The value is used for SPF calculation.

Use the no parameter with this command to set default metric to the default.

**Command Syntax**

`isis metric METRIC (level-1 | level-2)`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>METRIC</td>
<td>Specify a default metric.</td>
<td>1-16777214</td>
</tr>
<tr>
<td>level-1</td>
<td>Specify default metric for level-1 circuit.</td>
<td>-</td>
</tr>
<tr>
<td>level-2</td>
<td>Specify default metric for level-2 circuit.</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

By default, uses 10 for the metric value and the value is applied to both level-1 and level-2.

**Usage**

If neither the level-1 nor the level-2 keyword is configured, it applies to both levels.

**Examples**

The following example shows how to set default metric for the interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# isis metric 20
```

**Related Commands**

None
6.8.35 isis network

Command Purpose

Use this command to change a broadcast interface network type to a point-to-point network type.
Use the no parameter with this command to revert to the default setting of a broadcast interface network type.

Command Syntax

isis network point-to-point
no isis network (point-to-point |)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>point-to-point</td>
<td>Specify a point-to-point network.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

This option is disabled by default.

Usage

None

Examples

The following example shows how to change a broadcast interface network type to a point-to-point network type:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# isis network point-to-point

Related Commands

None

6.8.36 isis password

Command Purpose

Use this command to set the authentication password of Hello PDU on the interface.
Use the no parameter to clear the password.
**Command Syntax**

```snippets
isis password PASSWORD (level-1 | level-2 |)
no isis password (level-1 | level-2 |)
no isis password PASSWORD (level-1 | level-2 |)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PASSWORD</td>
<td>Specify a password string.</td>
<td>Up to 254 characters</td>
</tr>
<tr>
<td>level-1</td>
<td>Specify a password for Level-1 hello PDUs.</td>
<td>-</td>
</tr>
<tr>
<td>level-2</td>
<td>Specify a password for Level-2 hello PDUs.</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

**Interface Configuration**

**Default**

By default, no password is configured; this applies to both level-1 and level-2.

**Usage**

If neither the level-1 nor the level-2 keywrod is configured, it applies to both levels.

**Examples**

The following example shows how to set the authentication password of Hello PDU on the interface:

```snippets
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# isis password mypassWORD level-1
```

**Related Commands**

None

6.8.37 isis priority

**Command Purpose**

Use this command to set the priority for LAN DIS election. This command changes the priority value in LAN Hello PDUs. A lower priority value is less preferred in DIS election, and a higher priority value is more preferred.

**Command Syntax**

```snippets
isis priority PRIORITY (level-1 | level-2 |)
```
no isis priority (level-1 | level-2 |)
no isis priority <0-127> (level-1 | level-2 |)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRIORITY</td>
<td>Priority value</td>
<td>0-127</td>
</tr>
<tr>
<td>level-1</td>
<td>Specify a priority for Level-1 hello PDUs.</td>
<td>-</td>
</tr>
<tr>
<td>level-2</td>
<td>Specify a priority for Level-2 hello PDUs.</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

**Interface Configuration**

**Default**

By default, uses 64 for the priority value, and the priority is applied to both level-1 and level-2.

**Usage**

If neither the level-1 nor the level-2 keywords is configured, it applies to both levels.

**Examples**

The following example shows how to set the priority for LAN DIS election:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# isis priority 127
```

**Related Commands**

None

**6.8.38  isis retransmit-interval**

**Command Purpose**

Use this command to set LSP retransmission interval.
Use the no parameter to set the interval to the default.

**Command Syntax**

```
isis retransmit-interval INTERVAL
no isis retransmit-interval
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>Specify an interval for retransmission of the same LSP in seconds.</td>
<td>0-65535</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

5 seconds.

Usage

None

Examples

The following example shows how to set LSP retransmission interval:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# isis retransmit-interval 10
Switch(config-if)# no isis retransmit-interval
```

Related Commands

None

6.8.39 isis tag

Command Purpose

Use this command to set the tag for link-state packets (LSPs) sent out advertising routes for networks directly connected to an interface. If you do not specify a parameter, then the tag value is set for level-1-2 boundary. Use the no parameter to unset the tag.

Command Syntax

```
isis tag TAG (level-1 | level-2)
no isis tag
```
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TAG</strong></td>
<td>Tag value.</td>
<td>1-4294967295</td>
</tr>
<tr>
<td><strong>level-1</strong></td>
<td>Specify the tag value for the level-1 boundary.</td>
<td>-</td>
</tr>
<tr>
<td><strong>level-2</strong></td>
<td>Specify the tag value for the level-2 boundary.</td>
<td>-</td>
</tr>
</tbody>
</table>

### Command Mode

**Interface Configuration**

### Default

This option is disabled by default.

### Usage

None

### Examples

The following example shows how to set the tag for link-state packets (LSPs) sent out advertising routes for networks directly connected to an interface:

Switch# configure terminal  
Switch(config)# interface eth-0-1  
Switch(config-if)# isis tag 500 level-1

### Related Commands

None

---

6.8.40 **ispf**

### Command Purpose

Use this command to enable incremental SPF for a routing process.  
Use the no parameter to disable incremental SPF from a routing process.

### Command Syntax

ispf  
ispf (level-1 | level-1-2 | level-2-only)  
no ispf
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-1</td>
<td>Act as level-1 only IS.</td>
<td>-</td>
</tr>
<tr>
<td>level-1-2</td>
<td>Act as level-1-2 IS.</td>
<td>-</td>
</tr>
<tr>
<td>level-2-only</td>
<td>Act as level-2 only IS.</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration

**Default**

None

**Usage**

None

**Examples**

The following example shows how to enable incremental SPF for a routing process:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# ispf level-1
```

**Related Commands**

None

6.8.41 is-type

**Command Purpose**

To configure the routing level for an instance of the Intermediate System-to-Intermediate System (IS-IS) routing process, use the is-type command in router configuration mode.

Use the no parameter to set the IS to the default.

**Command Syntax**

```
is-type (level-1 | level-1-2 | level-2-only )
no is-type
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-1</td>
<td>Act as level-1 only IS.</td>
<td>-</td>
</tr>
<tr>
<td>level-1-2</td>
<td>Act as level-1-2 IS.</td>
<td>-</td>
</tr>
<tr>
<td>level-2-only</td>
<td>Act as level-2 only IS.</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration
Default

By default, uses level-1-2 if there is no Level-2 instance nor a Level-1-2 instance. Otherwise, it uses level-1.

Usage

None

Examples

The following example shows how to configure the routing level for an ISIS instance:

Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# is-type level-1

Related Commands

None

6.8.42  lsp-gen-interval

Command Purpose

Use this command to set minimum interval before regenerating the same LSP. The smaller the interval, the faster the convergence. However, this setting might cause more frequent flooding.
Use the no parameter with this command to set the interval to the default.

Command Syntax

lsp-gen-interval INTERVAL
lsp-gen-interval (level-1 | level-2) <1-120>
no lsp-gen-interval

Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>Specify a minimum interval in seconds.</td>
<td>1-120</td>
</tr>
<tr>
<td>level-1</td>
<td>Specify an interval for Level-1 IS.</td>
<td>-</td>
</tr>
<tr>
<td>level-2</td>
<td>Specify an interval for Level-2 IS.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default
30 seconds for the interval and the interval is applied to both level-1 and level-2.

**Usage**

None

**Examples**

The following example shows how to set minimum interval before regenerating the same LSP:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# lsp-gen-interval 5
```

**Related Commands**

None

6.8.43 lsp-mtu

**Command Purpose**

Use this command to set LSP MTU in bytes.

Use the no parameter with this command to set the MTU to the default.

**Command Syntax**

```
lsp-mtu (level-1 | level-2 ) MTU
no lsp-mtu (level-1 | level-2 )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTU</td>
<td>Specify an MTU size</td>
<td>512-1492</td>
</tr>
<tr>
<td>level-1</td>
<td>Specify an interval for Level-1 IS.</td>
<td>-</td>
</tr>
<tr>
<td>level-2</td>
<td>Specify an interval for Level-2 IS.</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration

**Default**

None

**Usage**

If neither the level-1 nor the level-2 keyword is configured, it applies to both levels.
Examples

The following example shows how to set LSP MTU in bytes:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# lsp-mtu 555
```

Related Commands

None

6.8.44 lsp-refresh-interval

Command Purpose

Use this command to set the LSP refresh interval.
IP Infusion recommends making the lsp-refresh-interval smaller than max-lsp-lifetime value.
Use the no parameter to set the interval to the default value.

Command Syntax

lsp-refresh-interval INTERVAL
no lsp-refresh-interval

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>Specify an LSP refresh interval in seconds.</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

900 seconds.

Usage

None

Examples

The following example shows how to set the LSP refresh interval:

```
Switch# configure terminal
Switch(config)# router isis bb
```
Switch(config-router)# lsp-refresh-interval 600
Switch(config-router)# no lsp-refresh-interval

Related Commands

None

6.8.45 max-area-addresses

Command Purpose

Use this command to configure additional manual addresses for an IS-IS area.
Use the no parameter to disable the manual addresses.

Command Syntax

max-area-addresses NUMBER
no max-area-addresses

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>Specify the maximum area address that can be supported</td>
<td>3-127</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

3

Usage

None

Examples

The following example shows how to configure additional manual addresses for an IS-IS area:

Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# max-area-address 4

Related Commands

None
6.8.46 max-lsp-lifetime

Command Purpose

Use this command to set the maximum LSP lifetime. You must set max-lsp-lifetime greater than lsp-refreshinterval. Use the no parameter to set the lifetime to the default.

Command Syntax

max-lsp-lifetime LIFETIME
no max-lsp-lifetime

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIFETIME</td>
<td>Specify an maximum LSP lifetime in seconds.</td>
<td>350-65535</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

1200 seconds.

Usage

None

Examples

The following example shows how to set the maximum LSP lifetime:

Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# max-lsp-lifetime 1500

Related Commands

None

6.8.47 metric-style

Command Purpose

Use this command to configure the metric style. Use the no parameter to set the style to the default style, narrow.
**Command Syntax**

metric-style (narrow | wide | transition) (level-1 | level-1-2 | level-2 |)

metric-style (narrow | wide | transition) (level-1 | level-1-2 | level-2 |)

no metric-style (narrow | wide | transition) (level-1 | level-1-2 | level-2 |)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>narrow</td>
<td>Specify the old style of TLVs with narrow metric.</td>
<td>-</td>
</tr>
<tr>
<td>wide</td>
<td>Specify the new style of TLVs to carry wider metric.</td>
<td>-</td>
</tr>
<tr>
<td>transition</td>
<td>Accept both styles of TLVs during transition</td>
<td>-</td>
</tr>
<tr>
<td>level-1</td>
<td>Specify the level-1 metric style.</td>
<td>-</td>
</tr>
<tr>
<td>level-2</td>
<td>Specify the level-2 metric style.</td>
<td>-</td>
</tr>
<tr>
<td>level-1-2</td>
<td>Specify the level-1-2 metric style.</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration

**Default**

By default, uses narrow metric style for level 1 and 2.

**Usage**

None

**Examples**

The following example shows how to configure the metric style:

```bash
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# metric-style wide
```

**Related Commands**

None

**6.8.48 net**

**Command Purpose**

Use this command to configure an Intermediate System-to-Intermediate System (IS-IS) network entity title (NET) for the routing process, use the net command in router configuration mode. To remove a NET, use the no form of this command.

Use the no parameter to remove the NET.

**Command Syntax**

net NET

no net NET
Parameter | Parameter Description | Parameter Value
--- | --- | ---
NET | Specify a network entity title (NET) in 1 to 13 octets | In XX.XXXX. … .XXXXXX format

**Command Mode**

Router Configuration

**Default**

By default, does not configure a NET and routing is not enabled for the interface.

**Usage**

None

**Examples**

The following example shows how to configure an Intermediate System-to-Intermediate System (IS-IS) network entity title (NET) for the routing process:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# net 49.0000.0001.0002.0003.00
```

**Related Commands**

None

**6.8.49 passive-interface**

**Command Purpose**

Use this command to suppress routing updates on all interfaces or on a specified interface, which puts the interfaces into passive mode. To advertise passive prefixes in LSP, there is no need to have an interface configured with ip router isis. Enabling passive interface on an ISIS enabled interface disables ISIS on the interface and makes the interface passive.

Use the no parameter with this command to remove interfaces from passive mode

**Command Syntax**

```
passive-interface (IFNAME)
nopassive-interface (IFNAME)
```

Parameter | Parameter Description | Parameter Value
--- | --- | ---
IFNAME | Indicates an interface name. | Support physical/aggregation/loopback/vlan/tunnel ports
Command Mode
Router Configuration

Default
None

Usage
None

Examples

The following example shows how to suppress routing updates on a specified interface:

Switch# configure terminal
Switch(config)# router isis 100
Switch(config-router)# passive-interface eth-0-1

Related Commands
None

6.8.50 prc-interval-exp

Command Purpose
Use this command to configure exponential back-off delay between PRC calculations.
Use the no parameter to disable any set exponential back-off delay between PRC calculations.

Command Syntax
prc-interval-exp
prc-interval-exp EXP_MIN EXP_MAX
no prc-interval-exp

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXP_MIN</td>
<td>Set the minimum delay between receiving a change to PRC calculation in milliseconds.</td>
<td>0-2147483647</td>
</tr>
<tr>
<td>EXP_MAX</td>
<td>Set the maximum delay between receiving a change to PRC calculation in milliseconds.</td>
<td>0-2147483647</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration

Default
Minimum Delay 500ms, Maximum Delay 50000ms

Usage
None
Examples

The following example shows how to configure exponential back-off delay between PRC calculations:

```
Switch# configure terminal
Switch(config)# router isis
Switch(config-router)# prc-interval-exp 100 10000
```

Related Commands

None

6.8.51 redistribute

Command Purpose

Use this command to redistribute routes from another protocol into the ISIS routing table. Use the no parameter to disable this function.

Command Syntax

```
redistribute ( connected | static | rip | ospf | bgp ) ( metric METRIC | metrictype ( internal | external ) | level-1 | level-2 | level-1-2 | route-map ROUTE_MAP )
```

```
no redistribute ( connected | static | rip | ospf | bgp )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>connected</td>
<td>Redistribute connected routes.</td>
<td>-</td>
</tr>
<tr>
<td>static</td>
<td>Redistribute static routes.</td>
<td>-</td>
</tr>
<tr>
<td>rip</td>
<td>Redistribute RIP routes.</td>
<td>-</td>
</tr>
<tr>
<td>ospf</td>
<td>Redistribute OSPF routes.</td>
<td>-</td>
</tr>
<tr>
<td>bgp</td>
<td>Redistribute BGP routes.</td>
<td>-</td>
</tr>
<tr>
<td>metric</td>
<td>Specify the metric for redistributed routes.</td>
<td>-</td>
</tr>
<tr>
<td>METRIC</td>
<td>Specify the IS-IS default metric.</td>
<td>0-4261412864</td>
</tr>
<tr>
<td>metrictype</td>
<td>Specify the IS-IS exterior metric type for redistributed routes:</td>
<td>-</td>
</tr>
<tr>
<td>internal</td>
<td>Set IS-IS internal metric type.</td>
<td>-</td>
</tr>
<tr>
<td>external</td>
<td>Set IS-IS external metric type.</td>
<td>-</td>
</tr>
<tr>
<td>level-1</td>
<td>IS-IS Level-1 routes.</td>
<td>-</td>
</tr>
<tr>
<td>level-2</td>
<td>IS-IS Level-2 routes.</td>
<td>-</td>
</tr>
<tr>
<td>level-1-2</td>
<td>IS-IS Level-1 and Level-2 routes.</td>
<td>-</td>
</tr>
<tr>
<td>route-map</td>
<td>Specify a Route map reference.</td>
<td>-</td>
</tr>
<tr>
<td>ROUTE_MAP</td>
<td>Specify name of the route-map.</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

None
**Usage**

None

**Examples**

The following example shows how to redistribute routes from another protocol into the ISIS routing table:

Switch# configure terminal
Switch(config)# router isis A
Switch(config-router)# redistribute bgp metric 12

**Related Commands**

None

**6.8.52 redistribute isis**

**Command Purpose**

Use this command to redistribute reachability information from one level to the other level. If an distribute-list name is given with this command for an access list that does not exist, the routes are still redistributed.

Use the no parameter with this command to stop redistribution.

**Command Syntax**

redistribute isis level-1 into level-2
redistribute isis level-2 into level-1
redistribute isis level-1 into level-2 distribute-list ACL
redistribute isis level-2 into level-1 distribute-list ACL
no redistribute isis level-1 into level-2
no redistribute isis level-2 into level-1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-1</td>
<td>Specify an inter-area route level-1.</td>
<td>-</td>
</tr>
<tr>
<td>level-2</td>
<td>Specify an inter-area routes level-2.</td>
<td>-</td>
</tr>
<tr>
<td>into</td>
<td>Specify a from level-n level into level-m.</td>
<td>-</td>
</tr>
<tr>
<td>distribute-list</td>
<td>Indicate the distributed-list parameter.</td>
<td>-</td>
</tr>
<tr>
<td>ACL</td>
<td>Access-list name</td>
<td>Up to 40 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration
Address Family Configuration

**Default**

By default, redistributes selected level-1 routes into level-2
**Usage**

None

**Examples**

The following example shows how to redistributes level-2 routes into level-1:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# router isis bb</td>
<td></td>
</tr>
<tr>
<td>Switch(config-router)# redistribute isis level-2 into level-1</td>
<td></td>
</tr>
</tbody>
</table>

**Related Commands**

None

**6.8.53 router isis**

**Command Purpose**

Use this command in global configuration mode to enable the Intermediate System-to-Intermediate System (IS-IS) routing protocol and to specify an IS-IS process. To disable IS-IS routing, use the noform of this command.

Use the no parameter with this command to disable IS-IS routing.

**Command Syntax**

```
router isis ( INSTANCE | )
no router isis ( INSTANCE | )
```

**Parameter** | **Parameter Description** | **Parameter Value**
--- | --- | ---
INSTANCE | Specify an ISO routing instance tag. | Up to 20 characters

**Command Mode**

Global Configuration

**Default**

None

**Usage**

None
Examples

The following example shows how to set ISIS instance name and create it:

Switch# configure terminal
Switch(config)# router isis New

Related Commands

None

6.8.54 set-overload-bit

Command Purpose

To configure the router to signal other routers not to use it as an intermediate hop in their shortest path first (SPF) calculations, use the set-overload-bit command in router configuration mode. To remove the designation, use the noform of this command.

Command Syntax

set-overload-bit { ( { suppress ( external | interlevel | external interlevel | interlevel external ) | on-startup ( TIME | wait-for-bgp ) ) | )
no set-overload-bit

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>suppress</td>
<td>Specify to suppress specific types of IP prefixes.</td>
<td>-</td>
</tr>
<tr>
<td>external</td>
<td>Specify to redistribute external reachability (to prevent the IP prefixes learned from other protocols from being advertised).</td>
<td>-</td>
</tr>
<tr>
<td>interlevel</td>
<td>Specify to redistribute interlevel reachability.</td>
<td>-</td>
</tr>
<tr>
<td>on-startup</td>
<td>Specify an interval in seconds after which the overload state is exited.</td>
<td>-</td>
</tr>
<tr>
<td>TIME</td>
<td>Specify the time in seconds to advertise oneself as overloaded after reboot.</td>
<td>5-86400</td>
</tr>
<tr>
<td>wait-for-bgp</td>
<td>Specify that BGP determines when to unset the overload bit.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

By default, no overload-bit is set.
Usage

None

Examples

The following example shows how to set overload bit:

Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# set-overload-bit

Related Commands

None

6.8.55 spf-interval-exp

Command Purpose

Use this command to set the minimum and maximum hold intervals between Shortest Path First (SPF) calculations. The spf-interval-exp command configures the minimum and maximum interval time between the receipt of a topology change and the calculation of the SPF. Use the no parameter with this command to set the minimum and maximum hold intervals to the default.

Command Syntax

spf-interval-exp EXP_MIN EXP_MAX
spf-interval-exp (level-1 | level-2 ) <0-2147483647> <0-2147483647>
no spf-interval-exp

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXP_MIN</td>
<td>Specify the minimum delay between receiving a change to the SPF calculation in milliseconds.</td>
<td>0-2147483647</td>
</tr>
<tr>
<td>EXP_MAX</td>
<td>Specify the maximum delay between receiving a change to the SPF calculation in milliseconds.</td>
<td>0-2147483647</td>
</tr>
<tr>
<td>level-1</td>
<td>Specify an interval for Level-1 IS.</td>
<td>-</td>
</tr>
<tr>
<td>level-2</td>
<td>Specify an interval for Level-2 IS.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

By default, uses 500 milliseconds and 50,000 milliseconds for the minimum and maximum hold intervals, respectively. The values are applied to both level-1 and level-2 if the level parameter is omitted.

Usage
Examples

The following example shows how to set the minimum and maximum hold intervals between Shortest Path First (SPF) calculations:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# spf-interval-exp level-1 600 60000
Switch(config-router)# no spf-interval-exp level-1
```

Related Commands

None

6.8.56 summary-address

Command Purpose

Use this command to configure Summary Address to summarize IPv4 reachability information. Use the no parameter with this command to unconfigure the summary.

Command Syntax

```
summary-address IP_ADDR/IP_MASK_LEN { level-1 | level-1-2 | level-2 } [ ( metric ) ( METRIC ) ]
```

```
o no summary-address IP_ADDR/IP_MASK_LEN
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR/IP_MASK_LEN</td>
<td>Specify the IPv4 prefix to be announced. IPv4 Address and mask length in A.B.C.D/M format</td>
<td></td>
</tr>
<tr>
<td>level-1</td>
<td>Specify the reachability information only for Level-1.</td>
<td>-</td>
</tr>
<tr>
<td>level-1-2</td>
<td>Specify the reachability information for both Level-1 and Level-2.</td>
<td>-</td>
</tr>
<tr>
<td>level-2</td>
<td>Specify the reachability information only for Level-2.</td>
<td>-</td>
</tr>
<tr>
<td>metric</td>
<td>Specify the metric for the summarized address.</td>
<td>-</td>
</tr>
<tr>
<td>METRIC</td>
<td>Specify the metric. The default is 0.</td>
<td>1-4294967295</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

By default, does not configure the summary-address. Summary-address is applied to Level-2 IS if level parameter is omitted.

Usage

If neither the level-1 nor the level-2 keyword is configured, it applies to level-2
Examples

The following example shows how to configure ipv4 Summary Address:

Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# summary-address 10.10.0.0/16

Related Commands

None

6.8.57 summary-prefix

Command Purpose

Use this command to configure the summary prefix to summarize IPv6 reachability information.
Use the no parameter to unconfigure the summary.

Command Syntax

summary-prefix GLOBAL_PREFIX/IPV6_MASK_LEN ( level-1 | level-1-2 | level-2 ) ( metric METRIC )
no summary-prefix GLOBAL_PREFIX/IPV6_MASK_LEN

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLOBAL_PREFIX/IPV6_MASK_LEN</td>
<td>Specify the IPv6 prefix to be announced.</td>
<td>IPv4 Address and mask length in X:X::X:X/M format</td>
</tr>
<tr>
<td>level-1</td>
<td>Specify the reachability information only for Level-1.</td>
<td>-</td>
</tr>
<tr>
<td>level-1-2</td>
<td>Specify the reachability information for both Level-1 and Level-2.</td>
<td>-</td>
</tr>
<tr>
<td>level-2</td>
<td>Specify the reachability information only for Level-2.</td>
<td>-</td>
</tr>
<tr>
<td>metric</td>
<td>Specify the metric for the summarized address.</td>
<td>-</td>
</tr>
<tr>
<td>METRIC</td>
<td>Specify the metric. The default is 0.</td>
<td>1-4294967295</td>
</tr>
</tbody>
</table>

Command Mode

Address Family Configuration

Default

By default, does not configure the summary-prefix. Summary-prefix is applied to Level-2 IS if level parameter is omitted.

Usage
If neither the level-1 nor the level-2 keysword is configured, it applies to level-2.

**Examples**

The following example shows how to configure ipv6 Summary Prefix:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# address-family ipv6
Switch(config-router-af)# summary-prefix 3ffe:1234::/32
```

**Related Commands**

None

**6.8.58 show clns is-neighbors**

**Command Purpose**

Use this command to display all IS neighbor adjacencies.

**Command Syntax**

```
show clns is-neighbors ( detail )
show clns INSTANCE is-neighbors ( detail )
show clns is-neighbors IFNAME ( detail )
show clns INSTANCE is-neighbors IFNAME ( detail )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE</td>
<td>Display information for specified instance.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Display information about a single interface.</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
<tr>
<td>detail</td>
<td>Display detailed information for all interfaces.</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None
Examples

The following example shows how to display all IS neighbor adjacencies:

Switch# show clns is-neighbors

Area 100:

<table>
<thead>
<tr>
<th>System Id</th>
<th>Interface</th>
<th>State</th>
<th>Type</th>
<th>Priority</th>
<th>Circuit Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.0000.0002</td>
<td>vlan100</td>
<td>Up</td>
<td>L2</td>
<td>64</td>
<td>0000.0000.0001.01</td>
</tr>
<tr>
<td>0000.0000.0002</td>
<td>vlan200</td>
<td>Up</td>
<td>L2</td>
<td>64</td>
<td>0000.0000.0001.02</td>
</tr>
</tbody>
</table>

Related Commands

None

6.8.59 show debugging isis

Command Purpose

Use this command to display the status of the debugging of the ISIS system.

Command Syntax

show debugging isis

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display the status of the debugging of the ISIS system:

Switch# show debugging isis

IS-IS debugging status:
  IS-IS spf debugging is on
Related Commands

None

6.8.60  show ip isis route

Command Purpose

Use this command to display IS-IS routing table for IPv4.

Command Syntax

show ip isis (INSTANCE | ) route

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE</td>
<td>Display information for specified instance.</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display IS-IS routing table for IPv4.:

Switch# show ip isis route

Related Commands

None

6.8.61  show ipv6 isis route

Command Purpose
Use this command to display the IS-IS routing table for IPv6.

**Command Syntax**

```
show ipv6 isis (INSTANCE | ) route
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE</td>
<td>Display information for specified instance.</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

The following example shows how to display IS-IS routing table for IPv6:

```
Switch# show ipv6 isis route
```

**Related Commands**

None

**6.8.62  show ipv6 isis topology**

**Command Purpose**

Use this command to display the IS-IS topology for IPv6.

**Command Syntax**

```
show ipv6 isis topology (l1 | l2 | level-1 | level-2 |)
show ipv6 isis INSTANCE topology (l1 | l2 | level-1 | level-2 |)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE</td>
<td>Display information for specified instance.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>l1</td>
<td>IS-IS level-1 SPF topology.</td>
<td>-</td>
</tr>
<tr>
<td>l2</td>
<td>IS-IS level-2 SPF topology.</td>
<td>-</td>
</tr>
<tr>
<td>level-1</td>
<td>IS-IS level-1 SPF topology.</td>
<td>-</td>
</tr>
<tr>
<td>level-2</td>
<td>IS-IS level-2 SPF topology.</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC
**Default**

None

**Usage**

None

**Examples**

The following example shows how to display the IS-IS topology for IPv6:

```plaintext
Switch# show ipv6 isis topology
```

**Related Commands**

None

---

**6.8.63 show ipv6 protocols isis**

**Command Purpose**

Use this command to display IPv6 process parameters and statistics.

**Command Syntax**

```
show ipv6 protocols isis
```

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

The following example shows how to display IPv6 process parameters and statistics:

```plaintext
```
Switch# show ipv6 protocols isis

Routing Protocol is "isis 2"
    Redistributing:
        Area Address(es):
    Distance: (default is 115)
Routing Protocol is "isis 1"
    Redistributing:
        Area Address(es):
    Distance: (default is 115)

Related Commands
None

6.8.64 show isis counter

Command Purpose
Use this command to display the IS-IS system counter entry MIBs.

Command Syntax
show isis counter

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following example shows how to display the IS-IS system counter entry MIBs:
Switch# show isis counter

Area b:
IS-IS Level-1 isisSystemCounterEntry:
<table>
<thead>
<tr>
<th>Counter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>isisSysStatCorrLSPs</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatAuthTypeFails</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatAuthFails</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatLSPDbaseOloads</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatManAddrDropFromAreas</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatAttemptToExMaxSeqNums</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatSeqNumSkips</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatOwnLSPPurges</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatIDFieldLenMismatches</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatMaxAreaAddrMismatches</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatPartChanges</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatSPFRuns</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatPRCRuns</td>
<td>0</td>
</tr>
</tbody>
</table>

**Area bb:**

IS-IS Level-1

<table>
<thead>
<tr>
<th>Counter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>isisSysStatCorrLSPs</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatAuthTypeFails</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatAuthFails</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatLSPDbaseOloads</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatManAddrDropFromAreas</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatAttemptToExMaxSeqNums</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatSeqNumSkips</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatOwnLSPPurges</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatIDFieldLenMismatches</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatMaxAreaAddrMismatches</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatPartChanges</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatSPFRuns</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatPRCRuns</td>
<td>0</td>
</tr>
</tbody>
</table>

IS-IS Level-2

<table>
<thead>
<tr>
<th>Counter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>isisSysStatCorrLSPs</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatAuthTypeFails</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatAuthFails</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatLSPDbaseOloads</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatManAddrDropFromAreas</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatAttemptToExMaxSeqNums</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatSeqNumSkips</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatOwnLSPPurges</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatIDFieldLenMismatches</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatMaxAreaAddrMismatches</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatPartChanges</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatSPFRuns</td>
<td>0</td>
</tr>
<tr>
<td>isisSysStatPRCRuns</td>
<td>0</td>
</tr>
</tbody>
</table>
Related Commands

None

6.8.65  show isis database

Command Purpose

Use this command to display detailed link state database information.

Command Syntax

show isis database
show isis database ( l1 | l2 | level-1 | level-2 ) LSPID ( detail | verbose )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>IS-IS link state database detailed information.</td>
<td>-</td>
</tr>
<tr>
<td>verbose</td>
<td>IS-IS link state database detailed information.</td>
<td>-</td>
</tr>
<tr>
<td>LSPID</td>
<td>LSPID in the form of XXXX.XXXX.XXXX.XX-XX.</td>
<td>-</td>
</tr>
<tr>
<td>l1</td>
<td>IS-IS level-1 link state database.</td>
<td>-</td>
</tr>
<tr>
<td>l2</td>
<td>IS-IS level-2 link state database.</td>
<td>-</td>
</tr>
<tr>
<td>level-1</td>
<td>IS-IS level-1 link state database.</td>
<td>-</td>
</tr>
<tr>
<td>level-2</td>
<td>IS-IS level-2 link state database.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display detailed link state database information.:

Switch# show isis database verbose

Area (null):
IS-IS Level-1 Link State Database:
LSPID    LSP Seq Num    LSP Checksum    LSP Holdtime    ATT/P/OL
0000.0000.0001.00-00* 0x00000002 0x9E50 1140 0/0/0

IS-IS Level-2 Link State Database:
LSPID    LSP Seq Num    LSP Checksum    LSP Holdtime    ATT/P/OL
0000.0000.0001.00-00* 0x00000003 0x9C51 1176 0/0/0

Related Commands
None

6.8.66 show isis interface

Command Purpose
Use this command to display detailed interface information.

Command Syntax
show isis interface
display isis interface IFNAME
display isis interface counter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Display the name of interface</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
<tr>
<td>counter</td>
<td>Display the interface counters.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following example shows how to display detailed interface information about ISIS:
Switch# show isis interface eth-0-1
eth-0-1 is up, line protocol is up

Routing Protocol: IS-IS ((null))

Network Type: Broadcast
Circuit Type: level-1-2
Local circuit ID: 0x01
Extended Local circuit ID: 0x00000001
Local SNPA: e6f5.41de.3200
IP interface address:
  1.1.1.1/24
IPv6 interface address:
  Level-1 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.01
  Number of active level-1 adjacencies: 0
  Level-1 LSP MTU: 1492
  Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.01
  Number of active level-2 adjacencies: 0
  Level-2 LSP MTU: 1492
  Next IS-IS LAN Level-1 Hello in 238 milliseconds
  Next IS-IS LAN Level-2 Hello in 238 milliseconds

Related Commands

None

6.8.67 show isis topology

Command Purpose

Use this command to display data about IS-IS topology.

Command Syntax

show isis topology ( l1 | l2 | level-1 | level-2 | )
show isis INSTANCE topology ( l1 | l2 | level-1 | level-2 | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE</td>
<td>Display information for specified instance.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>l1</td>
<td>Display the path to all level-1 routers in the area.</td>
<td>-</td>
</tr>
<tr>
<td>l2</td>
<td>Display the path to all level-2 routers in the domain.</td>
<td>-</td>
</tr>
<tr>
<td>level-1</td>
<td>Display the path to all level-1 routers in the area.</td>
<td>-</td>
</tr>
<tr>
<td>level-2</td>
<td>Display the path to all level-2 routers in the domain.</td>
<td>-</td>
</tr>
</tbody>
</table>
**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

The following example shows how to display data about IS-IS topology:

```
Switch# show isis topology
```

**Related Commands**

None

### 6.8.68 show running-config interface isis

**Command Purpose**

Use this command to display the ISIS interface configurations.

**Command Syntax**

```
show running-config interface IFNAME isis
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Display the name of interface.</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None
Usage

None

Examples

The following example shows how to display the ISIS interface configurations:

Switch# show running-config interface eth-0-1 isis

Building configuration...

interface eth-0-1
  ip router isis

Related Commands

None

6.8.69 show running-config router isis

Command Purpose

Use this command to display router ISIS configurations.

Command Syntax

show running-config router isis

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

None
The following example shows how to display router ISIS configurations:

Switch# show running-config router isis

Building configuration...
!
router isis
  net 10.0000.0000.0001.00

Related Commands

None
Chapter 7 IPv6 Routing Commands

7.1 OSPFv3 Commands

7.1.1 area default-cost

Command Purpose

To specify a cost for the default summary route sent into a stub, use the area default-cost command in router configuration mode. To remove the assigned default route cost, use the no form of this command.

Command Syntax

area AREA-ID default-cost COST
no area AREA-ID default-cost

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AREA-ID</td>
<td>Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address</td>
<td>IP address or number in the range of 0-4294967295</td>
</tr>
<tr>
<td>COST</td>
<td>Cost for the default summary route used for a stub.</td>
<td>0-16777215</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

The cost value is 1 by default.

Usage

The command is used only on an Area Border Router (ABR) attached to a stub. There are two stub area router configuration commands: the stub and default-cost options of the area command. In all routers and access servers attached to the stub area, the area should be configured as a stub area using the stub option of the area command. Use the default-cost option only on an ABR attached to the stub area. The default-cost option provides the metric for the summary default route generated by the ABR into the stub area.

Examples

The following example assigns a default cost of 20 to stub network 10.0.0.0:
Switch# configure terminal
Switch(config)#router ipv6 ospf 201
Switch(config-router)#area 10.0.0.0 stub
Switch(config-router)#area 10.0.0.0 default-cost 20

Related Commands

None

7.1.2 area range

Command Purpose

To consolidate and summarize routes at an area boundary, use the area range command in router configuration mode. To disable this function, use the no form of this command.

Command Syntax

area AREA-ID range ADDRESS/PREFIX-LENGTH ( advertise | not-advertise )
no area AREA-ID range ADDRESS/PREFIX-LENGTH
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AREA-ID</td>
<td>Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address</td>
<td>IP address or number in the range of 0-4294967295</td>
</tr>
<tr>
<td>ADDRESS</td>
<td>IPv6 address</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>PREFIX-LENGTH</td>
<td>Prefix length of the address</td>
<td>1-128</td>
</tr>
<tr>
<td>advertise</td>
<td>Advertise this range (default)</td>
<td>-</td>
</tr>
<tr>
<td>not-advertise</td>
<td>Do Not Advertise this range</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

**Router Configuration**

**Default**

This command is disabled by default.

**Usage**

The area range command is used only with Area Border Routers (ABRs). It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This behavior is called route summarization.

Multiple area router configuration commands specifying the range option can be configured. Thus, OSPF can summarize addresses for many different sets of address ranges.

**Examples**

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on area 10:

```
Switch# configure terminal
Switch(config)# router ipv6 ospf 201
Switch(config-router)# area 10 range 2004::1/16
```

**Related Commands**

None

**7.1.3 area stub**

**Command Purpose**

To define an area as a stub area, use the area stub command in router configuration mode.

To disable this function, use the no form of this command.

**Command Syntax**

```
area AREA-ID stub ( no-summary | )
no area AREA-ID stub ( no-summary | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AREA-ID</td>
<td>Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address</td>
<td>IP address or number in the range of 0-4294967295</td>
</tr>
<tr>
<td>no-summary</td>
<td>(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

**Router Configuration**
**Default**

No stub area is defined.

**Usage**

You must configure the area stub command on all routers and access servers in the stub area. Use the area router configuration command with the default-cost keyword to specify the cost of a default internal router sent into a stub area by an ABR.

There are two stub area router configuration commands: the stub and default-cost options of the area router configuration command. In all routers attached to the stub area, the area should be configured as a stub area using the stub keyword of the area command. Use the default-cost keyword only on an ABR attached to the stub area. The default-cost keyword provides the metric for the summary default route generated by the ABR into the stub area.

To further reduce the number of link-state advertisements (LSAs) sent into a stub area, you can configure the no-summary keyword on the ABR to prevent it from sending summary LSAs (LSA type 3) into the stub area.

**Examples**

The following example assigns a default cost of 20 to stub network 10.0.0.0:

```
Switch# configure terminal
Switch(config)# router ipv6 ospf 201
Switch(config-router)# area 10.0.0.0 stub
Switch(config-router)# area 10.0.0.0 default-cost 20
```

**Related Commands**

None

**7.1.4 auto-cost**

**Command Purpose**

To control how Open Shortest Path First Version3 (OSPFv3) calculates default metrics for the interface; use the auto-cost command in router configuration mode.

To assign cost based only on the interface type, use the no form of this command.

**Command Syntax**

```
auto-cost reference-bandwidth RATE
no auto-cost reference-bandwidth
```

**Parameter | Parameter Description | Parameter Value**

| RATE | Rate in Mbps (bandwidth). The default is 100 | 1 - 4294967 Mbps |

**Command Mode**

Router Configuration

**Default**

100 Mbps

**Usage**

The value set by the ipv6 ospf cost command overrides the cost resulting from the auto-cost command.

**Examples**

The following example changes the cost of the cost link to 1GBps:

```
Switch# configure terminal
Switch(config)# router ipv6 ospf 1
Switch(config-router)# auto-cost reference-bandwidth 1000
```

**Related Commands**

ipv6 ospf cost
7.1.5 clear ipv6 ospf

Command Purpose
To clear routing information based on the Open Shortest Path First (OSPF) routing process ID, use the clear ipv6 ospf command in privileged EXEC mode.

Command Syntax

```
clear ipv6 ospf (PID |)
```

Parameter | Parameter Description | Parameter Value
---|---|---
PID | (Optional) Process ID | 0-65535

Command Mode
Privileged EXEC

Default
None

Usage
Use the PID argument to clear only one OSPFv3 process. If the PID argument is not specified, all OSPFv3 processes are cleared.

Examples
The following example clears all OSPFv3 processes:
```
Switch# clear ipv6 ospf process
```

Related Commands
None

7.1.6 default-information originate (OSPFV3)

Command Purpose
To generate a default external route into an Open Shortest Path First Version3 (OSPFv3) routing domain, use the default-information originate command in router configuration mode.
To disable this feature, use the no form of this command.

Command Syntax

```
default-information originate
```

```
default-information originate { metric METRIC | metric-type TYPE | route-map ROUTE_MAP | always }
```

```
no default-information originate
```

```
no default-information originate { metric | metric-type | route-map | always }
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>always</td>
<td>(Optional) Always advertises the default route regardless of whether the system has a default route</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>METRIC</td>
<td>metric-value (Optional) Metric used for generating the default route. If you omit a value and do not specify a value using the default-metric router configuration command, the default metric value is 10. The value used is specific to the protocol</td>
<td>0-16777214</td>
</tr>
<tr>
<td>TYPE</td>
<td>(Optional) External link type associated with the default route advertised into the OSPF routing domain. It can be one of the following values</td>
<td>1,2</td>
</tr>
<tr>
<td>ROUTE_MAP</td>
<td>Route map reference</td>
<td>-</td>
</tr>
</tbody>
</table>
Command Mode
Router Configuration

Default
This command is disabled by default.

Usage
Whenever you use the redistribute or the default-information router configuration command to redistribute routes into an OSPFv3 routing domain, the switch automatically becomes an autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a default route into the OSPFv3 routing domain. The system still must have a default route for itself before it generates one, except when you have specified the always keyword.

Examples
The following example specifies a metric of 100 for the default route redistributed into the OSPFv3 routing domain and an external metric type of Type 1:

Switch# configure terminal
Switch(config)# router ipv6 ospf 109
Switch(config-router)# redistribute rip metric 100
Switch(config-router)#default-information originate metric 100 metric-type 1

Related Commands
redistribute (OSPFv3)

7.1.7 default-metric (OSPFv3)

Command Purpose
To set default metric values for the Open Shortest Path First Version3 (OSPFv3) routing protocol, use the default-metric command in router configuration mode. To return to the default state, use the no form of this command.

Command Syntax
default-metric METRIC-VALUE
no default-metric (METRIC-VALUE)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>METRIC-VALUE</td>
<td>Default metric value appropriate for the specified routing protocol.</td>
<td>0-16777214</td>
</tr>
<tr>
<td></td>
<td>Default metric value appropriate for the specified routing protocol.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Built-in, automatic metric translations, as appropriate for each routing protocol. The</td>
<td></td>
</tr>
<tr>
<td></td>
<td>metric of redistributed connected and static routes is set to 0</td>
<td></td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration

Default
default-metric is 20

Usage
The default-metric command is used in conjunction with the redistribute router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with
incompatible metrics. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

Examples

The following example shows a router in an autonomous system using both the Routing Information Protocol (RIPng) and the OSPFv3 routing protocols. The example advertises OSPFv3-derived routes using RIPng and assigns the Internal Gateway Protocol (IGP)-derived routes a RIPng metric of 10:

```
Switch# configure terminal
Switch(config)# router ipv6 ospf
Switch(config-router)# default-metric 10
Switch(config-router)# redistribute ripng
```

Related Commands

redistribute (OSPFv3)

7.1.8 distance (OSPFv3)

Command Purpose

To define Open Shortest Path First Version3 (OSPFv3) route administrative distances based on route type, use the distance command in router configuration mode.

To restore the default value, use the no form of this command.

Command Syntax

```
distance { DISTANCE | ospfv3 [ external DIST1 ] [ inter-area DIST2 ] [ intra-area DIST3 ] }
no distance { DISTANCE | ospfv3 }
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISTANCE</td>
<td>Administrative distance.</td>
<td>1-254.(routes with a distance value of 255 are not installed in the routing table)</td>
</tr>
<tr>
<td>external DIST1</td>
<td>(Optional) Sets the distance for routes from other routing domains, learned by redistribution. Range is 1 to 255. The default value is 110</td>
<td>1-254</td>
</tr>
<tr>
<td>inter-area DIST2</td>
<td>(Optional) Sets the distance for all routes from one area to another area. Range is 1 to 255. The default value is 110</td>
<td>1-254</td>
</tr>
<tr>
<td>intra-area DIST3</td>
<td>(Optional) Sets the distance for all routes within an area. Range is 1 to 255. The default value is 110</td>
<td>1-254</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

DIST1: 110
DIST2: 110
DIST3: 110

Usage

You may specify one of the keywords or use distance only to apply to all types of routes. The distance command allows you to set a distance for an entire group of routes, rather than a specific route that passes an access list.
A common reason to use the distance command is when you have multiple OSPFv3 processes with mutual redistribution, and you want to prefer internal routes from one over external routes from the other.

**Examples**

The following example shows a router in autonomous system using both the Routing Information Protocol (RIPng) and the OSPFv3 routing protocols. The example advertises OSPFv3-derived routes using RIPng and assigns the Internal Gateway Protocol (IGP)-derived routes a RIPng distance of 90:

```
Switch# configure terminal
Switch(config)# router ipv6 ospf
Switch(config-router)#distance 90
Switch(config-router)# redistribute ripng
```

**Related Commands**

None

7.1.9 distribute-list (OSPFv3)

**Command Purpose**

To filter networks received in updates or suppress networks from being advertised in updates, use the distribute-list command in router configuration mode. To cancel this function, use the no form of this command.

**Command Syntax**

distribute-list ACCESSS-LIST-NAME ( in | out ( bgp | connected | ospfv3 | ripng | static ) )

no distribute-list ACCESSS-LIST-NAME ( in | out ( bgp | connected | ospfv3 | ripng | static ) )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCESSS-LIST-NAME</td>
<td>Name of an access list to be applied</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>in</td>
<td>Filter networks received in updates</td>
<td>-</td>
</tr>
<tr>
<td>out</td>
<td>Suppress networks from being advertised in updates</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration

**Default**

This command is disabled by default.

**Usage**

This command must specify an access list.

**Examples**

In the following example, OSPFv3 process 1 is configured to accept two prefixes, prefix 2001:1:1::1/32 and prefix 3001:1:1::1/32:

```
Switch# configure terminal
Switch(config)# ipv6 access-list filter-as-router
Switch(config-ip-acl)# permit any 2001:1:1::1/32 any
Switch(config-ip-acl)# permit any 3001:1:1::1/32 any
Switch(config-ip-acl)# deny any any any
Switch(config)# router ipv6 ospf 1
Switch(config-router)# distribute-list acl1 in
```

**Related Commands**

ipv6 access-list
7.1.10 enable db-summary-opt

**Command Purpose**
Use this command to enable optimize the process when building ospfv3 neighbor ship.

**Command Syntax**

```
enable db-summary-opt
no enable db-summary-opt
```

**Command Mode**
Router Configuration

**Default**
Disable

**Usage**
After this function enabled, if the router receives a DD packet which has newer LSA, the router should delete the LSA in the database summary list, and should not send this LSA to its neighbor.

**Examples**
The following example enables this optimization:
```
Switch# configure terminal
Switch(config)# router ipv6 ospf 1
Switch(config-if)# enable db-summary-opt
Switch# configure terminal
Switch(config)# router ipv6 ospf 1
Switch(config-router)# enable db-summary-opt
```

**Related Commands**
None

7.1.11 ipv6 ospf cost

**Command Purpose**
To explicitly specify the cost of sending a packet on an interface, use the ipv6 ospf cost command in interface configuration mode. To reset the path cost to the default value, use the no form of this command.

**Command Syntax**

```
ipv6 ospf cost INTERFACE-COST ( instance ID | )
no ipv6 ospf cost ( instance ID | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERFACE-COST</td>
<td>Unsigned integer value expressed as the link-state metric.</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

**Command Mode**
Interface Configuration

**Default**
No default cost is predefined.

**Usage**
You can set the metric manually using this command, if you need to change the default. Using the bandwidth command changes the link cost as long as this command is not used. The link-state metric is advertised as the link cost in the router link advertisement.
In general, the path cost is calculated using the following formula:
Reference Bandwidth / bandwidth

Examples
The following example sets the interface cost value to 65:
```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 ospf cost 65
```

Related Commands
auto-cost reference bandwidth

7.1.12 ipv6 ospf dead-interval

Command Purpose
To set the interval during which at least one hello packet must be received from a neighbor before the router declares that neighbor down, use the ipv6 ospf dead-interval command in interface configuration mode. To restore the default value, use the no form of this command.

Command Syntax
```
ipv6 ospf dead-interval SECONDS (instance ID )
no ipv6 ospf dead-interval (instance ID )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>Interval (in seconds) during which the router must receive at least one hello packet from a neighbor or else that neighbor is removed from the peer list and does not participate in routing. The value must be the same for all nodes on the network.</td>
<td>1-65535</td>
</tr>
<tr>
<td>ID</td>
<td>Instance ID, the default value is 0.</td>
<td>0-255</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
The neighbor is considered as dead in 40s by default.

Usage
The dead interval is advertised in OSPFv3 hello packets. This value must be the same for all networking devices on a specific network. Specifying a smaller dead interval (seconds) will give faster detection of a neighbor being down and improve convergence, but might cause more routing instability.

Examples
The following example sets the OSPFv3 dead interval to 20 seconds:
```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 ospf dead-interval 20
```

Related Commands
ipv6 ospf hello-interval
show ipv6s ospf interface
7.1.13 ipv6 ospf hello-interval

Command Purpose
To specify the interval between hello packets that the switch sends on the interface, use the ip ospf hello-interval command in interface configuration mode. To return to the default time, use the no form of this command.

Command Syntax
```
ip ospf hello-interval SECONDS ( instance ID | )
nosp ospf hello-interval ( instance ID | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>Interval (in seconds) during which the router must receive at least one hello packet from a neighbor or else that neighbor is removed from the peer list and does not participate in routing. The value must be the same for all nodes on the network</td>
<td>1-65535</td>
</tr>
<tr>
<td>ID</td>
<td>Instance ID, the default value is 0.</td>
<td>0-255</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
10 seconds (Ethernet)
30 seconds (non-broadcast)

Usage
This value is advertised in the hello packets. The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

Examples
The following example sets the interval between hello packets to 15 seconds:
```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 ospf hellow-interval 15
```

Related Commands
ipv6 ospf dead-interval

7.1.14 ipv6 ospf mtu-ignore

Command Purpose
To disable Open Shortest Path First Version3 (OSPFv3) maximum transmission unit (MTU) mismatch detection on receiving Database Descriptor (DBD) packets, use the ipv6 ospf mtu-ignore command in interface configuration mode. To reset to default, use the no form of this command.

Command Syntax
```
ip ospf mtu-ignore ( instance ID | )
nosp ospf mtu-ignore ( instance ID | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Instance ID, the default value is 0.</td>
<td>0-255</td>
</tr>
</tbody>
</table>
Command Mode
Interface Configuration

Default

OSPFv3 MTU mismatch detection is enabled.

Usage

OSPFv3 checks whether neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange DBD packets. If the receiving MTU in the DBD packet is higher than the IP MTU configured on the incoming interface, OSPFv3 adjacency will not be established.

Examples

The following example disables MTU mismatch detection on receiving DBD packets:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 ospf mtu-ignore
```

Related Commands

None

7.1.15  ipv6 ospf priority

Command Purpose

To set the router priority, which helps determine the designated router for this network, use the ip ospf priority command in interface configuration mode.

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

Command Syntax

```
ipv6 ospf priority NUMBER-VALUE (instance ID | )  
no ipv6 ospf priority (instance ID | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER-VALUE</td>
<td>A number value that specifies the priority of the router.</td>
<td>0-255</td>
</tr>
<tr>
<td>ID</td>
<td>Instance ID, the default value is 0.</td>
<td>0-255</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

Priority of 1

Usage

When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the designated router or backup designated router. Router priority is configured only for interfaces to multi-access networks (in other words, not to point-to-point networks).

This priority value is used when you configure Open Shortest Path First Version3 (OSPFv3) for non-broadcast networks using the neighbor router configuration command for OSPFv3.

Examples

The following example sets the router priority value to 4:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 ospf priority 4
```
Related Commands

None

7.1.16 ipv6 ospf retransmit-interval

Command Purpose

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface, use the ipv6 ospf retransmit-interval command in interface configuration mode.

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

Command Syntax

ipv6 ospf retransmit-interval SECONDS (instance ID | )
no ipv6 ospf retransmit-interval (instance ID | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>Time (in seconds) between retransmissions. It must be greater than the expected round-trip delay between any two routers on the attached network.</td>
<td>1-65535 seconds</td>
</tr>
<tr>
<td>ID</td>
<td>Instance ID, the default value is 0.</td>
<td>0-255</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

5 seconds

Usage

When a router sends an LSA to its neighbor, it keeps the LSA until it receives back the acknowledgment message. If the router receives no acknowledgment, it will resend the LSA. The setting of this parameter should be conservative, or needless retransmission will result. The value should be larger for serial lines and virtual links.

Examples

The following example sets the retransmit interval value to 8 seconds:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 ospf retransmit-interval 8

Related Commands

None

7.1.17 ipv6 ospf transmit-delay

Command Purpose

To set the estimated time required to send a link-state update packet on the interface, use the ipv6 ospf transmit-delay command in interface configuration mode. To return to the default value, use the no form of this command.

Command Syntax

ipv6 ospf transmit-delay SECONDS (instance ID | )
no ipv6 ospf transmit-delay (instance ID | )
### transitive delay

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>Time (in seconds) between retransmissions. It must be greater than the expected round-trip delay between any two routers on the attached network.</td>
<td>1-65535 seconds</td>
</tr>
<tr>
<td>ID</td>
<td>Instance ID, the default value is 0.</td>
<td>0-255</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

1 second

**Usage**

Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the seconds argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface. If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low-speed links.

**Examples**

The following example sets the retransmit delay value to 3 seconds:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 ospf transmit-delay 3
```

**Related Commands**

None

### passive-interface (OSPF)

**Command Purpose**

To disable sending routing updates for the Open Shortest Path First Version 3 (OSPFv3) on an interface, use the `passive-interface` command in router configuration mode. To re-enable the sending of routing updates, use the `no` form of this command.

**Command Syntax**

```
passive-interface IFNAME
no passive-interface IFNAME
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>The interface name</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration

**Default**

Routing updates are sent on the interface.

**Usage**

If you disable the sending of routing updates on an interface, the particular subnet will continue to be advertised to other interfaces, and updates from other switches on that interface continue to be received and processed.
Examples

The following example sets the interface eth-0-1 as passive:
```
Switch# configure terminal
Switch(config)# router ipv6 ospf 200
Switch(config-router)# passive-interface eth-0-1
```

Related Commands

router ipv6 ospf

7.1.19 redistribute (OSPFv3)

Command Purpose

To redistribute routes from one routing domain into Open Shortest Path First Version3 (OSPFv3) routing domain, use the redistribute command in router configuration mode. To disable redistribution, use the no form of this command.

Command Syntax

```
redistribute PROTOCOL [ route-map WORD ] [ tag TAG-VALUE ] [ metric METRIC-VALUE ] [ metric-type TYPE-VALUE ]
```

```
no redistribute PROTOCOL [ metric METRIC-VALUE ] [ metric-type TYPE-VALUE ]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-map WORD</td>
<td>Route map name</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>PROTOCOL</td>
<td>(Optional) The name of a routing protocol, or the keyword connected, or static. If you specify a routing protocol, use one of the following keywords: bgp and ripng</td>
<td>connected/static/bgp/ripng</td>
</tr>
<tr>
<td>tag TAG-VALUE</td>
<td>Set tag for routes redistributed into OSPF</td>
<td>0-4294967295</td>
</tr>
<tr>
<td>metric METRIC-VALUE</td>
<td>(Optional) When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified</td>
<td>0-16777214</td>
</tr>
<tr>
<td>metric-type TYPE-VALUE</td>
<td>For OSPF, the external link type associated with the default route advertised into the OSPF routing domain. It can be one of two values</td>
<td>1-2</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

Route redistribution is disabled.
metric metric-value: 20
metric-type TYPE-VALUE: Type 2 external route

Usage

The metric value specified in the redistribute command supersedes the metric value specified using the default-metric command.
**Examples**

The following example redistribute the static routes into OSPFv3 with metric 10:
```
Switch# configure terminal
Switch(config)# router ospf 119
Switch(config-router)# redistribute static metric 10
```

**Related Commands**

default-metric

### 7.1.20 router-id (OSPF)

**Command Purpose**

To use a fixed router ID, use the router-id command in router configuration mode.
To force Open Shortest Path First Version3 (OSPFv3) use the previous OSPF router ID behavior, use the no form of this command.

**Command Syntax**

```
router-id IP-ADDRESS
no router-id
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-ADDRESS</td>
<td>Router ID in IP address format</td>
<td>IPv6 Address</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration

**Default**

No OSPF routing process is defined.

**Usage**

You can configure an arbitrary value in the IP address format for each router. However, each router ID must be unique.
If this command is used on an OSPFv3 router process which is already active (has neighbors), the new router-ID is used at the next reload or at a manual OSPFv3 process restart. To manually restart the OSPFv3 process, use the clear ip ospf command.

**Examples**

The following example specifies a fixed router-id:
```
Switch# configure terminal
Switch(config)# router ipv6 ospf 119
Switch(config-router)# router-id 10.1.1.1
```

**Related Commands**

clear ipv6 ospf
router ipv6 ospf

### 7.1.21 router ipv6 ospf

**Command Purpose**

To configure an Open Shortest Path First Version3 (OSPFv3) routing process, use the router ipv6 ospf command in global configuration mode. To terminate an OSPFv3s routing process, use the no form of this command.

**Command Syntax**

```
router ipv6 ospf [PROCESS-ID ]
no router ipv6 ospf [PROCESS-ID ]
```
**Parameter** | **Parameter Description** | **Parameter Value**
---|---|---
**PROCESS-ID** | Internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process | 1-65535

**Command Mode**

Global Configuration

**Default**

No OSPF routing process is defined.

**Usage**

You can specify multiple OSPFv3 routing processes in each router. If you do not specify the process-id, the process-id will be the default 0.

**Examples**

The following example configures an OSPFv3 routing process and assigns a process number of 109:

```bash
Switch# configure terminal
Switch(config)# router ipv6 ospf 109
```

**Related Commands**

None

**7.1.22 summary-address (OSPFv3)**

**Command Purpose**

To create aggregate addresses for Open Shortest Path First Version3 (OSPFv3), use the summary-address command in router configuration mode. To restore the default, use the no form of this command.

**Command Syntax**

```bash
summary-address PREFIX / PREFIX-LENGTH [ not-advertise ] [ tag TAG-VALUE ]
no summary-address PREFIX / PREFIX-LENGTH [ not-advertise ] [ tag TAG-VALUE ]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PREFIX</td>
<td>IP route prefix for the destination</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>PREFIX-LENGTH</td>
<td>Prefix length for the network</td>
<td>1-128</td>
</tr>
<tr>
<td>not-advertise</td>
<td>(Optional) Suppress routes that match the specified prefix/mask pair. This keyword applies to OSPFv3 only</td>
<td></td>
</tr>
<tr>
<td>tag TAG-VALUE</td>
<td>Route tag value</td>
<td>0-4294967295</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration

**Default**

This command is disabled by default.

**Usage**

Routes learned from other routing protocols can be summarized. The metric used to advertise the summary is the largest metric of all the more specific routes. This command helps reduce the size of the routing table.
Using this command for OSPFv3 causes an OSPFv3 Autonomous System Boundary Router (ASBR) to advertise one external route as an aggregate for all redistributed routes that are covered by the address. For OSPFv3, this command summarizes only routes from other routing protocols that are being redistributed into OSPFv3. Use the area range command for route summarization between OSPF areas. OSPFv3 does not support the summary-address 0.0.0.0/0 command.

Examples

In the following example, the summary address 2001:1:1::/48 includes address 2001:1:1:1::/64, 2001:1:1:2::/64, and so on. Only the address 2001:1:1::/48 is advertised in an external link-state advertisement:

Switch# configure terminal
Switch(config)# router ipv6 ospf
Switch(config-router)# summary-address 2001:1:1::/48

Related Commands
area range

7.1.23 show ipv6 ospf

Command Purpose
To display general information about Open Shortest Path First Version3 (OSPFv3) routing processes, use the show ipv6 ospf command in user EXEC or privileged EXEC mode.

Command Syntax

show ipv6 ospf (PROCESS-ID | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROCESS-ID</td>
<td>Internally used identification parameter for an OSPFv3 routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPFv3 routing process</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following is sample output from the show ipv6 ospf command when entered without a specific OSPFv3 process ID:

Switch# show ipv6 ospf 65535

Routing Process "OSPFv3 (65535)" with ID 1.1.1.1
  Process uptime is 1 hour 52 minutes
  SPF schedule delay min 0.500 secs, SPF schedule delay max 50.0 secs
  Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
  Number of incoming current DD exchange neighbors 0/5
  Number of outgoing current DD exchange neighbors 0/5
  Number of external LSA 0, Checksum Sum 0x0000
  Number of AS-Scoped Unknown LSA 0
  Number of LSA originated 3
  Number of LSA received 19
  Number of areas in this router is 1
  Area BACKBONE(0)
    Number of interfaces in this area is 1(1)
    SPF algorithm executed 6 times
    Number of LSA 4, Checksum Sum 0x16569
    Number of Unknown LSA 0
Related Commands

None

7.1.24 show ipv6 ospf database

Command Purpose

To display lists of information related to the Open Shortest Path First Version3 (OSPFv3) database for a specific router, use the show ip ospf database command in EXEC mode.

Command Syntax

show ipv6 ospf { PROCESS-ID | } database
show ipv6 ospf { PROCESS-ID | } database adv-router ROUTER-ID
show ipv6 ospf { PROCESS-ID | } database ( external | inter-prefix | inter-router | intra-prefix | link | network | router ) { ( LINK-STATE-ID | self-originate )
show ipv6 ospf { PROCESS-ID | } database max-age
show ipv6 ospf { PROCESS-ID | } database self-originate

Parameter | Parameter Description | Parameter Value
--- | --- | ---
PROCESS-ID | Internally used identification parameter for an OSPFv3 routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPFv3 routing process | 1-65535
adv-router ROUTER-ID | (Optional) Displays all the LSAs of the specified router. If no IP address is included, the information is about the local router itself (in this case, the same as self-originate) | IPv4 Address in A.B.C.D format
LINK-STATE-ID | (Optional) Portion of the Internet environment that is being described by the advertisement. The value entered depends on the advertisement’s LS type. It must be entered in the form of an IP address | IPv4 Address in A.B.C.D format

Command Mode

Privileged EXEC

Default

None

Usage

The various forms of this command deliver information about different OSPFv3 link state advertisements.

Examples

The following is sample output from the show ipv6 ospf database command when no arguments or keywords are used:
Switch# show ipv6 ospf 65535 database

| OSPFv3 Router with ID (1.1.1.1) (Process 65535) |
| Link-LSA (Interface vlan1000) |
| Link State ID | ADV Router | Age | Seq# | CkSum | Prefix |
| 0.0.19.232 | 1.1.1 | 1492 | 0x80000000 | 0xlim3e3 | 1 |
| 0.0.19.232 | 2.2.2.2 | 1488 | 0xlim0000002 | 0xlim94 | 1 |
| Router-LSA (Area 0.0.0.0) |
Related Commands

None

7.1.25 show ipv6 ospf interface

Command Purpose

To display Open Shortest Path First Version3 (OSPFv3)-related interface information; use the show ipv6 ospf interface command in EXEC mode.

Command Syntax

show ipv6 ospf interface (IFNAME )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>(Optional) Interface name. If the interface-name argument is included, only information for the specified interface is included</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output of the show ipv6 ospf interface command when vlan12 is specified:

```
Switch# show ipv6 ospf interface vlan 12

vlan12 is up, line protocol is up
  Interface ID 4108
  IPv6 Prefixes
    fe80::db5d5ff:fed9:ff00/10 (Link-Local Address)
    2004:12:0:12:1/96
  OSPFV3 Process (0), Area 0.0.0.0, Instance ID 0
    Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
    Transmit Delay is 1 sec, State Backup, Priority 1
  Designated Router (ID) 2.2.2.2
    Interface Address fe80::188f:beff:fe99:9800
    Backup Designated Router (ID) 1.1.1.1
    Interface Address fe80::be5d5ff:fed9:ff00
    Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
    Neighbor Count is 1, Adjacent neighbor count is 1
```

Related Commands

None
7.1.26  show ipv6 ospf neighbor

Command Purpose
To display Open Shortest Path First Version3 (OSPFv3)-neighbor information on a per-interface basis, use the show ipv6 ospf neighbor command in privileged EXEC mode.

Command Syntax
show ipv6 ospf neighbor (IFNAME |) (NEIGHBOR-ID |) (detail |)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>(Optional) Interface name. If the interface-name argument is included, only information for the specified interface is included.</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports.</td>
</tr>
<tr>
<td>NEIGHBOR-ID</td>
<td>(Optional) Neighbor ID IPv4 Address in A.B.C.D format</td>
<td>-</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays all neighbors given in detail (lists all neighbors).</td>
<td></td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following is sample output from the show ipv6 ospf neighbor command showing a single line of summary information for each neighbor:

Switch# show ipv6 ospf neighbor

OSPFv3 Process (0)
Neighbor ID Pri State Dead Time Interface Instance ID
2.2.2.2 1  Full/DR 00:00:31 vlan12 0
2.2.2.2 1  Full/DR 00:00:33 vlan1212 0

OSPFv3 Process (65535)
Neighbor ID Pri State Dead Time Interface Instance ID
2.2.2.2 1  Full/DR 00:00:31 vlan1000 0

Related Commands
None

7.1.27  show ipv6 ospf database database-summary

Command Purpose
To display the summary of database used by OSPFv3, use the show ip ospf database database-summary command in privileged EXEC mode.

Command Syntax
show ipv6 ospf (PROCESS-ID |) database database-summary
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROCESS-ID</td>
<td>(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPF routing process</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

The following example shows how to use show ipv6 ospf database database-summary command:

```
Switch# show ipv6 ospf 65535 database database-summary
```

<table>
<thead>
<tr>
<th>LSA Type</th>
<th>Count</th>
<th>MaxAge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Network</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Inter-Prefix</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Inter-Router</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Intra-Prefix</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Subtotal</td>
<td>4</td>
<td>0</td>
</tr>
</tbody>
</table>

**Related Commands**

None

7.1.28 show ipv6 ospf route

**Command Purpose**

To display the summary of routes used by OSPFv3, use the show ipv6 ospf route summary command in privileged EXEC mode.

**Command Syntax**

```
show ipv6 ospf (PROCESS-ID | ) route
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROCESS-ID</td>
<td>(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPFv3 routing process</td>
<td>1-65535</td>
</tr>
</tbody>
</table>
Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following example shows how to use `show ipv6 ospf route` command:

```
Switch# show ipv6 ospf route
```

| OSPFv3 Process (0) | Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area 
| Destination       | E1 - OSPF external type 1, E2 - OSPF external type 2 |
| Metric            |                                                          |
| C 2004:1:0:10::/96| directly connected, vlan10, Area 0.0.0.0               |
|                  | 1                                                        |
| C 2004:1:0:20::/96| directly connected, vlan20, Area 0.0.0.14               |
|                  | 1                                                        |
| C 2004:1:0:100::/96| directly connected, vlan100, Area 0.0.0.0              |
|                  | 1                                                       |
| C 2004:1:0:200::/96| directly connected, vlan200, Area 0.0.0.14             |
|                  | 1                                                       |
| O 2004:2:0:10::/96| via fe80::188f:beff:fe99:9800, vlan1212, Area 0.0.0.0 |
|                  | via fe80::188f:beff:fe99:9800, vlan12, Area 0.0.0.0    |
|                  | 2                                                       |
| IA 2004:2:0:20::/96| via fe80::188f:beff:fe99:9800, vlan1212, Area 0.0.0.0 |
|                  | via fe80::188f:beff:fe99:9800, vlan12, Area 0.0.0.0    |
|                  | 2                                                       |

Related Commands
None

### 7.1.29 show ipv6 ospf route summary

**Command Purpose**
To display the summary of routes used by OSPFv3, use the `show ipv6 ospf route summary` command in privileged EXEC mode.

**Command Syntax**
```
show ipv6 ospf route (PROCESS-ID | ) route summary
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROCESS-ID</td>
<td>(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPFv3 routing process</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC

**Default**
None
Usage
None

Examples
The following example shows how to use show ipv6 ospf route summary command:
Switch# show ipv6 ospf route summary

<table>
<thead>
<tr>
<th>OSPFv3 Router with ID (1.1.1.1) (Process ID 0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Type</td>
</tr>
<tr>
<td>(C) Connected</td>
</tr>
<tr>
<td>(D) Discard</td>
</tr>
<tr>
<td>(O) Intra area</td>
</tr>
<tr>
<td>(IA) Inter area</td>
</tr>
<tr>
<td>(E1) Ext type 1</td>
</tr>
<tr>
<td>(E2) Ext type 2</td>
</tr>
<tr>
<td>(N1) NSSA Ext type 1</td>
</tr>
<tr>
<td>(N2) NSSA Ext type 2</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

OSPFv3 Router with ID (1.1.1.1) (Process ID 65535)

| Route Type | Count |
| (C) Connected | 1 |
| (D) Discard | 0 |
| (O) Intra area | 1 |
| (IA) Inter area | 0 |
| (E1) Ext type 1 | 0 |
| (E2) Ext type 2 | 0 |
| (N1) NSSA Ext type 1 | 0 |
| (N2) NSSA Ext type 2 | 0 |
| Total | 2 |

Related Commands
None

7.1.30  show ipv6 protocols ospf

Command Purpose
To display IPv6 routing protocol process parameters and statistics of Open Shortest Path First Version3 (OSPFv3). Use the show ipv6 ospf protocols ospf command in privileged EXEC mode.

Command Syntax

```
show ipv6 protocols ospf
```

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following example shows how to use show ipv6 protocols ospf command:
Switch# show ipv6 protocols ospf

```
Routing Protocol is "OSPFv3 (0)" with ID 1.1.1.1
  Redistributing:
  Distance: (default is 110)
Routing Protocol is "OSPFv3 (65535)" with ID 1.1.1.1
```
Redistributing:
   Distance: (default is 110)

Related Commands
None

7.1.31 timers spf

Command Purpose
To turn on Open Shortest Path First Version3 (OSPFv3) shortest path first (SPF) throttling, use the timers spf command in router configuration mode. To turn off SPF throttling, use the no form of this command.

Command Syntax

```
timers spf exp SPF-HOLD_MIN SPF-HOLD_MAX
no timers spf exp
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPF-HOLD_MIN</td>
<td>Indicates the maximum hold time between two consecutive SPF calculations.</td>
<td>0-2147483647 milliseconds</td>
</tr>
<tr>
<td>SPF-HOLD_MAX</td>
<td>Indicates the minimum hold time between two consecutive SPF calculations.</td>
<td>0-2147483647 milliseconds</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration

Default
None

Usage
None

Examples

The following example shows how to configure SPF calculation parameters:
```
Switch# configure terminal
Switch(config)# router ipv6 ospf 1
Switch(config-router)# router-id 10.10.10.2
Switch(config-router)# timers spf exp 20 50
```

Related Commands
None

7.1.32 max-concurrent-dd

Command Purpose
To specify Maximum number allowed to process DD concurrently, use the max-concurrent-dd command in router configuration mode. To restore default value, use the no form of this command.

Command Syntax

```
max-concurrent-dd NUMBER-VALUE
no max-concurrent-dd
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER-VALUE</td>
<td>Number of DD process</td>
<td>1-65535</td>
</tr>
</tbody>
</table>
Command Mode

Router Configuration

Default

None

Usage

This command used to specify Maximum number allowed to process DD concurrently.

Examples

The following example shows how to use max-concurrent-dd command:

```
Switch# configure terminal
Switch(config)# router ipv6 ospf 100
Switch(config-router)# router-id 10.10.10.2
Switch(config-router)# max-concurrent-dd 10
```

Related Commands

None

7.1.33 debug ipv6 ospf

Command Purpose

Use this command to specify all debugging options for OSPFv3. Use the no parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf ( all | )
no debug ipv6 ospf ( all | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>enable all debugging</td>
<td></td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

The debug ospf all command enables the display of all debug information.

Examples

```
Switch# debug ipv6 ospf all
Switch# debug ipv6 ospf
```

Related Commands

None

7.1.34 debug ipv6 ospf events

Command Purpose

Use this command to specify debugging options for OSPFv3 event troubleshooting. Use this command without parameters to turn on all the options. Use the no parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf events ( abr | asbr | nssa | os | router | vlink )
no debug ipv6 ospf events ( abr | asbr | nssa | os | router | vlink )
```
### Parameter & Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>abr</td>
<td>shows ABR events</td>
<td>-</td>
</tr>
<tr>
<td>asbr</td>
<td>shows ASBR events</td>
<td>-</td>
</tr>
<tr>
<td>nssa</td>
<td>shows NSSA events</td>
<td>-</td>
</tr>
<tr>
<td>os</td>
<td>shows OS interaction events</td>
<td>-</td>
</tr>
<tr>
<td>router</td>
<td>shows others router events</td>
<td>-</td>
</tr>
<tr>
<td>vlink</td>
<td>shows virtual link events</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

The debug ospf event command enables the display of debug information related to OSPFv3 internal events.

**Examples**

Switch# debug ipv6 ospf events nssa  
Switch# debug ipv6 ospf events lsa

**Related Commands**

None

### 7.1.35 debug ipv6 ospf ifsm

**Command Purpose**

Use this command to specify debugging options for OSPFv3 Interface Finite State Machine (IFSM) troubleshooting. Use the no parameter with this command to disable this function.

**Command Syntax**

d debug ipv6 ospf ifsm ( status | events | timers )
no debug ipv6 ospf ifsm ( status | events | timers )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>Displays IFSM status information</td>
<td>-</td>
</tr>
<tr>
<td>events</td>
<td>Displays IFSM event information</td>
<td>-</td>
</tr>
<tr>
<td>timers</td>
<td>Displays IFSM TIMER information</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

The debug ospf ifsm command enables the display of debug information related to the Interface Finite State Machine (IFSM).

**Examples**

Switch# debug ipv6 ospf ifsm timers
Related Commands
None

7.1.36  debug ipv6 ospf nfsm

Command Purpose
Use this command to specify debugging options for OSPFv3 Neighbor Finite State Machine (NFSM) troubleshooting. Use the no parameter with this command to disable this function.

Command Syntax
debug ipv6 ospf nfsm (status | events | timers)
no debug ipv6 ospf nfsm (status | events | timers)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>Displays NFSM status information</td>
<td>-</td>
</tr>
<tr>
<td>events</td>
<td>Displays NFSM event information</td>
<td>-</td>
</tr>
<tr>
<td>timers</td>
<td>Displays NFSM TIMER information</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
The debug ospf nfsm command enables the display of debug information related to the Neighbor Finite State Machine (NFSM).

Examples
Switch# debug ipv6 ospf nfsm timers

Related Commands
None

7.1.37  debug ipv6 ospf lsa

Command Purpose
Use this command to specify debugging options for OSPFv3 Link State Advertisements (LSA) troubleshooting. Use the no parameter with this command to disable this function.

Command Syntax
debug ipv6 ospf lsa (flooding | generate | install | maxage | refresh)
no debug ipv6 ospf lsa (flooding | generate | install | maxage | refresh)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>flooding</td>
<td>Displays LSA flooding</td>
<td>-</td>
</tr>
<tr>
<td>generate</td>
<td>Displays LSA generate</td>
<td>-</td>
</tr>
<tr>
<td>install</td>
<td>Displays LSA installation</td>
<td>-</td>
</tr>
<tr>
<td>maxage</td>
<td>Displays the maximum age of LSA in seconds</td>
<td>-</td>
</tr>
<tr>
<td>refresh</td>
<td>Displays LSA refresh</td>
<td>-</td>
</tr>
</tbody>
</table>
**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
The `debug ospf lsu` command enables the display of debug information related to internal operations of LSAs.

**Examples**
```
Switch# debug ipv6 ospf lsu install
```

**Related Commands**
None

### 7.1.38 debug ipv6 ospf packet

**Command Purpose**
Use this command to specify debugging options for OSPFv3 packets. Use the `no` parameter with this command to disable this function.

**Command Syntax**
```
dbgv6 ospf packet PARAMETERS
no debug ipv6 ospf packet PARAMETERS
PARAMETERS = dd | detail | hello | ls-ack | ls-request | ls-update | recv | send
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dd</td>
<td>Specifies debugging for OSPF database descriptions</td>
<td>-</td>
</tr>
<tr>
<td>detail</td>
<td>Sets the debug option to detailed information</td>
<td>-</td>
</tr>
<tr>
<td>hello</td>
<td>Specifies debugging for OSPF hello packets</td>
<td>-</td>
</tr>
<tr>
<td>ls-ack</td>
<td>Specifies debugging for OSPF link state acknowledgments</td>
<td>-</td>
</tr>
<tr>
<td>ls-request</td>
<td>Specifies debugging for OSPF link state requests</td>
<td>-</td>
</tr>
<tr>
<td>ls-update</td>
<td>Specifies debugging for OSPF link state updates</td>
<td>-</td>
</tr>
<tr>
<td>recv</td>
<td>Specifies the debug option set for received packets</td>
<td>-</td>
</tr>
<tr>
<td>send</td>
<td>Specifies the debug option set for sent packets</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
The `debug ospf packet` command enables the display of debug information related to the sending and receiving of packets.

**Examples**
```
Switch# debug ipv6 ospf packet dd send detail
```

**Related Commands**
None
7.1.39 debug ipv6 ospf route

Command Purpose
Use this command to specify which route calculation to debug. Use this command without parameters to turn on all the options. Use the no parameter with this command to disable this function.

Command Syntax
debug ipv6 ospf route ( ase | ia | install | spf )
no debug ipv6 ospf route ( ase | ia | install | spf )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ase</td>
<td>Specifies the debugging of external route calculation</td>
<td>-</td>
</tr>
<tr>
<td>ia</td>
<td>Specifies the debugging of Inter-Area route calculation</td>
<td>-</td>
</tr>
<tr>
<td>install</td>
<td>Specifies the debugging of route installation</td>
<td>-</td>
</tr>
<tr>
<td>spf</td>
<td>Specifies the debugging of SPF calculation</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
The debug ospf route command enables the display of debug information related to route-calculation

Examples
Switch# debug ipv6 ospf route install

Related Commands
None

7.1.40 show debugging ipv6 ospf

Command Purpose
Use this command to display the set OSPFv3 debugging option..

Command Syntax
show debugging ipv6 ospf

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This is a sample output from the show debugging ipv6 ospf command. Some lines in this output wrap around, they might not wrap around in the actual display:
Switch# show debugging ipv6 ospf
OSPFv3 debugging status:
OSPFv3 all packet detail debugging is on
OSPFv3 all IFSM debugging is on
OSPFv3 all NFSM debugging is on
OSPFv3 all LSA debugging is on
OSPFv3 all route calculation debugging is on
OSPFv3 all event debugging is on

Related Commands
None

7.1.41 show resource ipv6 ospf

Command Purpose
Use this command to display the route resources used by OSPFv3 protocol.

Command Syntax
show resource ipv6 ospf

Command Mode
Privileged EXEC

Default
None

Usage
None.

Examples
The following is sample output from the show resource ipv6 ospf command:
Switch# show resource ipv6 ospf

<table>
<thead>
<tr>
<th>OSPFv3 Resource</th>
<th>Used</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routes</td>
<td>16</td>
<td>1913</td>
</tr>
</tbody>
</table>

Related Commands
show ipv6 ospf route summary
7.2 RIPng Commands

7.2.1 router ipv6 rip

Command Purpose

To enable or configure the Routing Information Protocol next generation (RIPng) routing process, use the router ipv6 rip command in global configuration mode. To disable the RIPng routing process, use the no form of this command.

Command Syntax

router ipv6 rip
no router ipv6 rip

Command Mode

Global Configuration

Default

No RIPng routing process is defined.

Usage

None

Examples

The following example shows how to enable RIPng routing process:

Switch# configure terminal
Switch(config)# router ipv6 rip

Related Commands

None

7.2.2 ipv6 router rip

Command Purpose

To enable RIPng routing process on specific interface, use the command ipv6 router rip in interface configuration mode. Use the no parameter with this command to disable RIPng routing process on interface.

Command Syntax

ipv6 router rip
no ipv6 router rip

Command Mode

Interface Configuration

Default

None.

Usage

None

Examples

The following example shows how to enable RIPng on the interface eth-0-1:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 router rip
Related Commands

None

7.2.3 ipv6 rip metric-offset

Command Purpose

Use this command to set RIP metric offset in interface mode.
To restore the default metric, use the no form of this command.

Command Syntax

ipv6 rip metric-offset NUMBER-VALUE
no ipv6 rip metric-offset NUMBER-VALUE

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER-VALUE</td>
<td>Metric offset value</td>
<td>1-16</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

Metric offset value is 1.

Usage

Metric offset value is used to add the metric of the network on which the message arrived (as the RFC describes).

Examples

The following example shows how to set metric offset as 2:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 rip metric-offset 2

Related Commands

None

7.2.4 ipv6 rip split-horizon

Command Purpose

To enable the split horizon mechanism for Routing Information Protocol next generation (RIPng), use the ipv6 rip split-horizon command in interface configuration mode.
To disable the split horizon mechanism, use the no form of this command.

Command Syntax

ipv6 rip split-horizon (poisoned | )
no ipv6 rip split-horizon

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>poisoned</td>
<td>Split horizon with poisoned reverse</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

This command is enabled with poisoned reverse by default.
Usage

In general, changing the default state for the ipv6 rip split-horizon command is not recommended, unless you are certain that your application requires a change in order to properly advertise routes.

Examples

The following example enables split horizon without poisoned reverse:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 rip split-horizon
```

Related Commands

None

7.2.5  default-information originate (RIPng)

Command Purpose

To generate a default route into Routing Information Protocol next generation (RIPng), use the default-information originate command in router configuration mode.
To disable this feature, use the no form of this command.

Command Syntax

default-information originate (route-map NAME | )
no default-information originate

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Route map name to reference</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

This command is disabled by default.

Usage

The default route can be learned by neighbor, but can't be stored in FIB.

Examples

The following example originates a default route (0::0/0) into RIPng:

```
Switch# configure terminal
Switch(config)# router ipv6 rip
Switch(config-router)# default-information originate
```

Related Commands

None

7.2.6  default-metric (RIPng)

Command Purpose

To specify the metrics to be assigned to redistributed routers for Routing Information Protocol next generation (RIPng), use the default-metric command in router configuration mode.
To return to the default state, use the no form of this command.

Command Syntax

default-metric NUMBER-VALUE
no default-metric
**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 RIPng and the Open Shortest Path First (OSPFv3) routing protocols. The example advertises OSPFv3-derived routes using RIPng and assigns the OSPFv3-derived routes a RIPng metric of 10:

```bash
Switch# configure terminal
Switch(config)# router ipv6 rip
Switch(config-router)# default-metric 10
Switch(config-router)# redistribute ospfv3
```

**Related Commands**

redistribute (RIPng)

---

### 7.2.7 distance (RIPng)

**Command Purpose**

To define an administrative distance for routes that are inserted into the routing table, use the distance command in router configuration mode.

To return the administrative distance to its default distance definition, use the no form of this command.

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual switch or a group of switches. Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value is, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

**Command Syntax**

distance DISTANCE

no distance

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISTANCE</td>
<td>Administrative distance</td>
<td>1-255. (routes with a distance value of 255 are not installed in the routing table)</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration

**Default**

By default, the distance is 120.
Usage

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Default Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected interface</td>
<td>0</td>
</tr>
<tr>
<td>Static route</td>
<td>1</td>
</tr>
<tr>
<td>External Border Gateway Protocol (eBGP)</td>
<td>20</td>
</tr>
<tr>
<td>Open Shortest Path First (OSPF)</td>
<td>110</td>
</tr>
<tr>
<td>Routing Information Protocol (RIP)/ Routing Information Protocol next generation (RIPng)</td>
<td>120</td>
</tr>
<tr>
<td>Internal BGP</td>
<td>200</td>
</tr>
<tr>
<td>Unknown</td>
<td>255</td>
</tr>
</tbody>
</table>

Examples

The following example set the distance of RIPng 200:
```
Switch# configure terminal
Switch(config)#router ipv6 rip
Switch(config-router)#distance 200
```

Related Commands

None

7.2.8 neighbor (RIPng)

Command Purpose

To specify a neighboring router to which to notify routing updating information, use the neighbor command in router configuration mode. To remove the neighbor, use the no form of this command.

Command Syntax

`neighbor IPv6_ADDR IFNAME`  
`no neighbor IP-ADDRESS IFNAME`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPV6_ADDR</td>
<td>Link-local IP address of a peer switch with which routing information will be notified</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Interface name to which the neighbor is specified</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

No neighboring switches are defined.

Usage

Especially use the neighbor command in conjunction with the passive-interface command to send routing updates to specific neighbors. This command permits the point-to-point (non-multicast) notification of routing update information. Multiple neighbors can be configured.

Examples

In the following example, RIPng updates are sent to all interfaces which have been enabled RIPng routing except eth-0-1. However, in this case a neighbor switch configuration command is included. This command permits the sending of routing updates to specific neighbors:
Switch# configure terminal
Switch(config)# router ipv6 rip
Switch(config-router)# passive-interface eth-0-1
Switch(config-router)# neighbor fe80:db8::1 eth-0-1

Related Commands
router rip

7.2.9 offset-list (RIPng)

Command Purpose
To add an offset to incoming and outgoing metrics to routes exchanging via Routing Information Protocol next generation (RIPng), use the offset-list command in router configuration mode.
To remove an offset list, use the no form of this command.

Command Syntax
offset-list ACCESSS-LIST-NAME (in | out) METRIC-OFFSET (IFNAME | )
no offset-list (in | out) (IFNAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCESSS-LIST-NAME</td>
<td>Named access list to be applied</td>
<td>Up to 40 characters</td>
</tr>
<tr>
<td>in</td>
<td>Applies the access list to incoming metrics</td>
<td>-</td>
</tr>
<tr>
<td>out</td>
<td>Applies the access list to outgoing metrics</td>
<td>-</td>
</tr>
<tr>
<td>METRIC-OFFSET</td>
<td>Positive offset to be applied to metrics for networks matching the access list. The metric-offset range is 0 to 16</td>
<td>0-16</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Interface name to which the offset list is applied</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration

Default
This command is configured by default.

Usage
Especially if the offset value is added to the routing metric by offset-list, the default action where the metric updates when RIPng message arrives (as RFC defined) is ignored, but outputs will be added.
The offset value is added to the routing metric. An offset list with an interface is considered extended and takes precedence over an offset list that is not extended. Therefore, if an entry passes the extended offset list and the normal offset list, the offset of the extended offset list is added to the metric.

Examples
In the following example, the switch applies an offset of 10 if access list 21 permits:
Switch# configure terminal
Switch(config)# router ipv6 rip
Switch(config-router)# offset-list 21 10

Related Commands
None
7.2.10 passive-interface (RIPng)

Command Purpose
To disable sending routing updates for the Routing Information Protocol next generation (RIPng) on an interface, use the passive-interface command in router configuration mode.
To enable the sending of routing updates, use the no form of this command.

Command Syntax
passive-interface IFNAME
no passive-interface IFNAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>The interface name</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration

Default
Interface is active by default.

Usage
The command disable the sending of routing updates and ignore the request message from neighbor on an interface, but updates from other routers on that interface should be received and processed.

Examples
The following example sets the interface eth-0-1 as passive:
Switch# configure terminal
Switch(config)# router ipv6 rip
Switch(config-router)# passive-interface eth-0-1

Related Commands
router ipv6 rip

7.2.11 redistribute (RIPng)

Command Purpose
To redistribute routes from one routing domain into RIPng routing domain, use the redistribute command in router configuration mode.
To disable redistribution, use the no form of this command.

Command Syntax
redistribute PROTOCOL [ metric VALUE ] | route-map NAME |
no redistribute PROTOCOL

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROTOCOL</td>
<td>The name of a routing protocol, or the keyword connected, or static. If you specify a routing protocol, use one of the following keywords: bgp, and ospfv3, static, connected, isis</td>
<td>connected/static/bgp/ospf/isis</td>
</tr>
<tr>
<td>metric VALUE</td>
<td>(Optional) When redistributing other routing process to the RIP process, the default metric is 1 if no metric value is specified</td>
<td>1-16</td>
</tr>
<tr>
<td>route-map NAME</td>
<td>Route map reference, name of route-map entry</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>
**Command Mode**

Router Configuration

**Default**

Route redistribution is disabled.
Metric-value: 1

**Usage**

The metric value specified in the redistribute command supersedes the metric value specified using the default-metric command.

**Examples**

The following example redistributes the static routes into RIPng with metric 10:

```
Switch# configure terminal
Switch(config)#router ipv6 rip
Switch(config-router)#redistribute static metric 10
```

**Related Commands**

default-metric

---

7.2.12 **timers basic (RIPng)**

**Command Purpose**

To adjust Routing Information Protocol next generation (RIPng) network timers, use the timers basic command in router configuration mode.
To restore the default timers, use the no form of this command.

**Command Syntax**

timers basic UPDATE TIMEOUT INVALID
no timers basic

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPDATE</td>
<td>Rate (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol</td>
<td>5-2147483647 seconds</td>
</tr>
<tr>
<td>TIMEOUT</td>
<td>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</td>
<td>5-2147483647 seconds</td>
</tr>
<tr>
<td>INVALID</td>
<td>Time after which an invalid route is removed from RIPng routing database</td>
<td>5-2147483647 seconds</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration

**Default**

Update timer: 30 seconds
Timeout timer: 180 seconds
Invalid timer: 120 seconds

**Usage**

The basic timing parameters for RIPng are adjustable. Because RIPng is executing a distributed, asynchronous routing algorithm, these timers must be the same for all switches and access servers in the network.
Examples

The following example sets updates to every 5 seconds. If a switch is not learned from in 15 seconds, the route is declared unusable. And after 15 seconds the invalid route will be removed from RIPng routing database:
Switch# configure terminal
Switch(config)#router ipv6 rip
Switch(config-router)#timers basic 5 15 15

Related Commands

None

7.2.13  distribute-list(RIPng)

Command Purpose

To filter networks in routing updates, use the distribute-list command in router configuration mode.
To restore the default value, use the no form of this command.

Command Syntax

distribute-list ( prefix NAME | ACCESSS-LIST-NAME ) ( in | out ) ( IFNAME )
no distribute-list ( prefix name | ACCESSS-LIST-NAME ) ( in | out ) ( IFNAME )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix NAME</td>
<td>Filter prefixes in routing update</td>
<td>Up to 40 characters</td>
</tr>
<tr>
<td>ACCESSS-LIST-NAME</td>
<td>Access-list name</td>
<td>Up to 40 characters</td>
</tr>
<tr>
<td>in</td>
<td>Filter incoming routing updates</td>
<td>-</td>
</tr>
<tr>
<td>out</td>
<td>Filter outgoing routing updates</td>
<td>-</td>
</tr>
<tr>
<td>IFNAME</td>
<td>The interface name</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

None

Usage

None

Examples

The following example filters the received RIPng routes:
Switch# configure terminal
Switch(config)#router ipv6 rip
Switch(config-router)# distribute-list prefix 1 in

Related Commands

ipv6 prefix-list

7.2.14  aggregate-address (RIPng)

Command Purpose

To specify an aggregate RIPng route announcement, use the aggregate-address command in router configuration mode.
To disable this feature, use the no form of this command.

Command Syntax

aggregate-address IPV6_PREFIX ( avoid-feedback | ) IFNAME
no aggregate-address IP-ADDRESS IFNAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPV6_PREFIX</td>
<td>Specify an aggregate network (IPv6 address prefix and length).</td>
<td>IPv6 Address and mask length in X:X::X:X/M format</td>
</tr>
<tr>
<td>avoid-feedback</td>
<td>Forbid to learn the address which is the same to aggregate address from the interface</td>
<td></td>
</tr>
<tr>
<td>IFNAME</td>
<td>The interface name</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration

**Default**

No aggregate address is defined.

**Usage**

If the routing info is suppressed by aggregate-address, it is still stored in RIPng database, but willn’t be notified to neighbor. On the other hand the aggregate-address will be notified to neighbor. The command only be useful when the interface is L3.

**Examples**

In the following example, RIPng specify an aggregate address into RIPng database:

```
Switch# configure terminal
Switch(config)#router ipv6 rip
Switch(config-router)# aggregate-address 2001:db8::/32
```

**Related Commands**

None

7.2.15 route map(RIPng)

**Command Purpose**

Use this command to set a route map for input or output filtering on a specified interface. Use the no parameter with this command to disable this function.

**Command Syntax**

```
route-map NAME (in | out ) IFNAME
no route-map name ( in | out ) IFNAME
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>route map name</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>in</td>
<td>route map for input filtering</td>
<td></td>
</tr>
<tr>
<td>out</td>
<td>route map for output filtering</td>
<td></td>
</tr>
<tr>
<td>IFNAME</td>
<td>Specify an interface name to which to associate the route map</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration

**Default**

None.
Usage
None

Examples
In the following example, set a route map for input filtering interface eth-0-1:
Switch# configure terminal
Switch(config)# router ipv6 rip
Switch(config-router)# route-map routemap10 in eth-0-1

Related Commands
None

7.2.16 maximum-prefix(RIPng)

Command Purpose
Use this command to configure the maximum prefix. Use the no parameter with this command to disable the limiting of the number of RIPng routes in the routing table.

Command Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER-VALUE</td>
<td>maximum number of RIPng routes allowed</td>
<td>1-65535</td>
</tr>
<tr>
<td>PERCENTAGE-VALUE</td>
<td>Percentage of maximum routes to generate a warning. The default threshold is 75%.</td>
<td>1-100</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration

Default
None.

Usage
Use this command to configure the maximum prefix.

Examples
In the following example, set maximum RIPng prefix is 700 and warning percentage is 70%:
Switch# configure terminal
Switch(config)# router ipv6 rip
Switch(config-router)# maximum-prefix 700 70

Related Commands
None

7.2.17 show ipv6 rip database

Command Purpose
Use this command to display RIPng information database.

Command Syntax
show ipv6 rip database

Command Mode
Privileged EXEC
Default
None

Usage
None

Examples
The following is sample output from the show ip rip database command:
Switch# show ipv6 rip database

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>If</th>
<th>Met Tag</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rc 2001:db8:0:6::/64</td>
<td>::</td>
<td>eth-0-9</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Rc 2001:db8:0:49::/64</td>
<td>::</td>
<td>eth-0-48</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Codes:
- R - RIP,
- Rc - RIP connected,
- Rs - RIP static,
- Ra - RIP aggregated,
- Rcx - RIP connect suppressed,
- Rsx - RIP static suppressed,
- K - Kernel,
- C - Connected,
- S - Static,
- O - OSPF,
- I - IS-IS,
- B - BGP

Related Commands
show ipv6 rip database

7.2.18  show ipv6 rip interface

Command Purpose
To display summary information of Routing Information Protocol next generation (RIPng) for a specific interface, use the show ip rip interface command in privileged EXEC mode.

Command Syntax
show ipv6 rip interface (IFNAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>The interface name</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following is sample output from the show ip rip interface command:
Switch# show ipv6 rip interface eth-0-9

eth-0-9 is up, line protocol is up
Routing Protocol: RIPng
  Passive interface: Disabled
  Split horizon: Enabled with Poisoned Reversed
IPv6 interface address:
  2001:db8:0:6::2/64
  fe80::b4df:82ff:fe70:ec00/10

Related Commands
show ipv6 rip database
7.2.19  show ipv6 rip database database-summary

Command Purpose
Use this command to display the summary statistics for RIPng database.

Command Syntax
show ipv6 rip database database-summary

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following is sample output from the show ip rip database database-summary command:
Switch# show ipv6 rip database database-summary

<table>
<thead>
<tr>
<th>Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIPng connected</td>
<td>2</td>
</tr>
<tr>
<td>Total</td>
<td>2</td>
</tr>
</tbody>
</table>

Related Commands
show ipv6 rip database

7.2.20  show ipv6 protocol rip

Command Purpose
To show Routing Information Protocol next generation (RIPng), use the show ipv6 protocol rip command in privileged EXEC mode.

Command Syntax
show ipv6 protocol rip

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following is sample output from the show ipv6 rip interface command:
Switch# show ipv6 protocol rip
Routing Protocol is "ripng"
Sending updates every 30 seconds with +/-50%, next due in 2949331570 seconds
Timeout after 180 seconds, garbage collect after 120 seconds
Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set
Default redistribute metric is 1
Redistributing:
Interface
eth-0-9
eth-0-48
Routing for Networks:
Number of routes (including connected): 2
Distance: (default is 120)

Related Commands
None

7.2.21  debug IPv6 rip

Command Purpose
Use this command to specify the options for the displayed debugging information for RIPng events, RIPng packets. Use the no parameter with this command to disable all debugging.

Command Syntax
ddebug ipv6 rip ( all | events | packet |)
nno debug ipv6 ( all | events | packet |)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>All RIPng debug information</td>
<td>-</td>
</tr>
<tr>
<td>events</td>
<td>RIPng events debug information is displayed</td>
<td>-</td>
</tr>
<tr>
<td>packet</td>
<td>packet (recv</td>
<td>send) (detail) Specifies RIPng packets only</td>
</tr>
<tr>
<td>recv</td>
<td>Debug switch for receiving packets</td>
<td>-</td>
</tr>
<tr>
<td>send</td>
<td>Debug switch for sending packets</td>
<td>-</td>
</tr>
<tr>
<td>detail</td>
<td>Debug switch for the detailed information of receiving or sending packets</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
Disabled

Usage
None

Examples
The following example displays information about the ripng packets that are received and sent out from the connected router:

Switch# debug ipv6 rip packet

Related Commands
show debugging rip

7.2.22  show debugging ipv6 rip

Command Purpose
Use this command to display the RIP debugging status for these debugging options: nsm debugging, RIP event debugging, RIP packet debugging.

Command Syntax
show debugging ipv6 rip

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
Use this command to display the debug status of RIPng.

**Examples**
The following is sample output from the show debugging ripng command:
```
Switch# show debugging ipv6 rip
RIPng debugging status:
  RIPng event debugging is on
```

**Related Commands**
debug ipv6 rip

7.2.23  show resource ipv6 rip

**Command Purpose**
Use this command to display the route resources used by RIPng protocol.

**Command Syntax**
```
show resource ipv6 rip
```

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
The following is sample output from the show resource ipv6 rip command:
```
Switch# show resource ipv6 rip
RIPng Resource Used Capability
Routes 2 728
```

**Related Commands**
show ipv6 rip database

7.2.24  clear ipv6 rip route

**Command Purpose**
To clear the specific route in RIPng routing table, use the command clear ipv6 rip route in privileged exec mode.

**Command Syntax**
clear ipv6 rip route (IPV6_PREFIX | connected | static | ospfv3 | bgp | all)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPV6_PREFIX</td>
<td>Removes entries which exactly match this destination address</td>
<td>X:X::X:X/M format</td>
</tr>
<tr>
<td></td>
<td>from the RIPng routing table.</td>
<td></td>
</tr>
<tr>
<td>connected</td>
<td>Removes entries for connected routes from the RIPng routing</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>table.</td>
<td></td>
</tr>
<tr>
<td>static</td>
<td>Removes static entries from the RIPng routing table.</td>
<td>-</td>
</tr>
<tr>
<td>ospfv3</td>
<td>Removes only OSPF routes from the RIPng routing table.</td>
<td>-</td>
</tr>
<tr>
<td>bgp</td>
<td>Removes only BGP routes from the RIPng routing table.</td>
<td>-</td>
</tr>
<tr>
<td>all</td>
<td>Removes the entire RIPng routing table.</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC

**Default**
None.

**Usage**
Use this command to clear specific data from the RIPng routing table.

**Examples**
In the following example, clear the entire RIPng routing table:
```
Switch# clear ipv6 rip route all
```

**Related Commands**
None.

### 7.3 IPv6UC Commands

#### 7.3.1 ipv6 enable

**Command Purpose**
Use this command to enable ipv6 function. Use the no form of this command to disable ipv6 function.

**Command Syntax**
```
ipv6 enable
no ipv6 enable
```

**Command Mode**
Global Configuration

**Default**
Ipv6 function is disabled by default.

**Usage**
This command is used to enable the ipv6 function globally. Ipv6 packet should be processed as a L2 packet when ipv6 function is disabled.

**Examples**
The following example shows how to enable IPv6:
Switch# configure terminal
Switch(config)# ipv6 enable

Related Commands
None

7.3.2 max-static-v6routes

Command Purpose
To configure the maximum ipv6 static routes in system, use the max-static-v6routes command in global configuration mode. To configure the maximum static routes to default value, use the no form of this command.

Command Syntax
max-static-v6routes COUNT
no max-static-v6routes

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>COUNT</td>
<td>The count of maximum ipv6 static routes.</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
Please reference the current TCAM profile.

Usage
Users should not configure the maximum ipv6 static routes more than system profile of FIB. Also, users should not configure the maximum ipv6 static routes less than the current static routes count.

Examples
The following example displays how to change maximum ipv6 static routes to 10:

Switch# configure terminal
Switch(config)# max-static-v6routes 10

Related Commands
show ipv6 route

7.3.3 ipv6 route

Command Purpose
To establish ipv6 static routes, use the ipv6 route command in global configuration mode. To remove ipv6 static routes, use the no form of this command.

Command Syntax
ipv6 route vrf NAME DEST_PREFIX (GLOBAL_PREFIX | LINK_LOCAL IFNAME | IFNULL | ADMIN_DISTANCE |) ipv6 route DEST_PREFIX (GLOBAL_PREFIX | LINK_LOCAL IFNAME | IFTUNNEL | IFNULL | ADMIN_DISTANCE |) no ipv6 route vrf NAME DEST_PREFIX (GLOBAL_PREFIX | LINK_LOCAL IFNAME | IFNULL |) no ipv6 route DEST_PREFIX (GLOBAL_PREFIX | LINK_LOCAL IFNAME | IFTUNNEL | IFNULL |)
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf NAME</td>
<td>VRF instance name</td>
<td>Up to 15 characters</td>
</tr>
<tr>
<td>DEST_PREFIX</td>
<td>IPv6 route prefix (in format X:X::X/X/M) for the destination</td>
<td>IPv6 Address and mask length in X:X::X/X/M format</td>
</tr>
<tr>
<td>GLOBAL_PREFIX</td>
<td>IPv6 route global unicast address (in format X:X::XX) for the nexthop</td>
<td>IPv6 Address in X:X::X format</td>
</tr>
<tr>
<td>LINK_LOCAL</td>
<td>IPv6 route link local address (FE80::/10) for the nexthop</td>
<td>IPv6 Address in X:X::X format</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Outgoing interface for the ipv6 route</td>
<td>Support physical/aggregation/vlan/tunnel ports</td>
</tr>
<tr>
<td>IFTUNNEL</td>
<td>Tunnel interface name for the ipv6 route</td>
<td>tunnel &lt;0-1023&gt;</td>
</tr>
<tr>
<td>IFNULL</td>
<td>null 0 interface for the ipv6 route</td>
<td>null 0</td>
</tr>
<tr>
<td>ADMIN_DISTANCE</td>
<td>(Optional) An administrative distance. The default administrative distance for a static route is 1. This configuration is optional.</td>
<td>1-255</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
There is not any static IPv6 route configured by default.

**Usage**
None

**Examples**
```
Switch# configure terminal
Switch(config)# ipv6 route 3001::1/64 fe80::1234 eth-0-2
Switch(config)# ipv6 route vrf a 3002::1/64 3001::1
```

**Related Commands**
show ipv6 route

### 7.3.4 ipv6 address

**Command Purpose**
To set an IPv6 address for an interface, use the ipv6 address command in interface configuration mode. To remove an IPv6 address, use the no form of this command.

**Command Syntax**
```
ipv6 address GOLBAL_FREFIX ( eui-64 | )
nov6 address GOLBAL_FREFIX ( eui-64 | )
ipv6 address LINK-LOCAL link-local
no ipv6 address LINK-LOCAL link-local
ipv6 address auto link-local
no ipv6 address auto link-local
no ipv6 address
```
### Command Mode

**Interface Configuration**

**Default**

There is not any ipv6 address on the interface by default.

**Usage**

Use this command to configure ipv6 address on the interface. Use the no form of this command to remove the ipv6 address. This configuration should not affect the ipv4 functions and other ipv6 configuration on the interface.

The maximum count of the Link-local address is 1; the maximum count of the global address address is 8.

Use this command with the keyword “auto link-local” to automatically generate a link-local address, if there is no link-local address on this interface. Use the no form of this command with the keyword “auto link-local” to remove the automatically generated link-local address, if there is only that automatically generated link-local address left on this interface.

Use this command with a specified ipv6 address (e.g. 3ffe:506::1/48) to configure a global unicast ipv6 address. Use this command with the keyword “eui-64” to generate interface id automatically by the eui-64 algorithm. The global address should not be same. Use the no form of this command the remove the specified ipv6 global unicast address.

If there is no link-local address on the interface, system should automatically generate one when configure a global unicast ipv6 address.

Use this command with a specified ipv6 address (e.g. fe80::1) and a keyword “link-local” to configure a link-local address. Use the no form of this command with the specified ipv6 address and the keyword “link-local” to remove the specified ipv6 link-local address. The specified link-local address has a higher priority than the automatically generated link-local address, that can overwrite the automatically generated one.

Use the no form of this command without any parameters or keywords to remove all ipv6 addresses on the interface, include ipv6 global addresses and link-local addresses.

**Examples**

The following example shows how to configure link local address and global unicast address:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 address fe80::1233
Switch(config-if)# ipv6 address 3001:1:1234/64
```

**Related Commands**

- `show ipv6 interface`

### 7.3.5 show ipv6 route

**Command Purpose**

Use this command to show the ipv6 routes.

**Command Syntax**

```
show ipv6 route (vrf NAME | ) (database | )
show ipv6 route (vrf NAME | ) (database | ) (bgp | connected | ospf | rip | static |)
show ipv6 route (vrf NAME | ) IPV6_ADDRESS
show ipv6 route (vrf NAME | ) IPV6_PREFIX
show ipv6 route (vrf NAME | ) summary
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPV6_PREFIX</td>
<td>IPv6 prefix in $XX:XX/M$ format</td>
<td>IPv6 Address and mask length in $XX:XX/M$ format</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

Use this command to show the ipv6 routes

**Examples**

The following example shows the result of this command:

Switch# show ipv6 route

IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP
[*] - [AD/Metric]
Timers: Uptime
S 3001::/64 [1/0]
   via fe80::1234, eth-0-2, 04:09:56
C 3001:1::/64
   via ::, eth-0-1, 01:39:07
C 3001:1::128/128
   via ::, eth-0-1, 01:39:07
S 3002::/64 [1/0]
   via 3001::1 (recursive via fe80::1234), eth-0-2, 04:09:19
C 3ffe:2::/64
   via ::, eth-0-2, 1d19h37m
S 3ffe:2::/64 [1/0]
   via ::, eth-0-2, 1d19h37m
S 3ffe:2::/128
   via ::, eth-0-2, 1d19h37m
S fe80::/10
   via ::, Null0, 1d19h53m

Switch# show ipv6 route database

IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP
[*] - [AD/Metric]
> - selected route, * - FIB route, p - stale info
Timers: Uptime
S > 3001::/64 [1/0]
   * via fe80::1234, eth-0-2, 04:10:45
C > 3001:1::/64
   * via ::, eth-0-1, 01:39:56
C > 3001:1::128/128
   * via ::, eth-0-1, 01:39:56
S > 3002::/64 [1/0]
   * via 3001::1 (recursive via fe80::1234), eth-0-2, 04:10:08
C > 3ffe:2::/64
   * via ::, eth-0-2, 1d19h37m
C > 3ffe:2::/128
   * via ::, eth-0-2, 1d19h37m
C > fe80::/10
   * via ::, Null0, 1d19h54m

Switch# show ipv6 route static

IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP
[*] - [AD/Metric]
Timers: Uptime
S 3001::/64 [1/0]
   via fe80::1234, eth-0-2, 04:11:42
Switch# show ipv6 route 3001::64
Routing entry for 3001::/64
  Known via "static", distance 1, metric 0, best
  Last update 04:12:32 ago
  * via fe80::1234, eth-0-2
Switch# show ipv6 route 3001::64/64
Routing entry for 3001::/64
  Known via "static", distance 1, metric 0, best
  Last update 04:13:03 ago
  * via fe80::1234, eth-0-2
Switch# show ipv6 route summary
IPv6 routing table name is Default-IPv6-Routing-Table(0)
IPv6 routing table maximum-paths is 8
 Route source networks
  connected 5
  static 2
  Total 7

Related Commands

ipv6 route

7.3.6 show ipv6 interface

Command Purpose

Use this command to show the ipv6 interface status on the interface.

Command Syntax

show ipv6 interface (IFNAME | brief)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>IPv6 interface status and configuration</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
<tr>
<td>brief</td>
<td>Brief summary of IPv6 status and configuration</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows the result of this command:
Switch# show ipv6 interface eth-0-1

Interface eth-0-1
  Interface current state: UP
  The maximum transmit unit is 1500 bytes
  IPv6 is enabled, link-local address is fe80::1233
Global unicast address(es):
  3001:1::1234, subnet is 3001:1::/64
Joined group address(es):
  ff02::ff00:1234
  ff02::ff00:0
  ff02::ff00:1233
  ff02::2
  ff02::1
ICMP error messages limited to one every 2000 milliseconds
ICMP redirects are always sent
ND DAD is enabled, number of DAD attempts: 1
ND router advertisement is disabled
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements max interval: 600 secs
ND router advertisements min interval: 198 secs
ND router advertisements live for 1800 seconds
ND router advertisements hop-limit is 0
Hosts use stateless autoconfig for addresses.

Switch # show ipv6 interface eth-0-1 brief
*down: administratively down

<table>
<thead>
<tr>
<th>Interface</th>
<th>Status</th>
<th>Protocol</th>
<th>IPv6 address</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-0-1</td>
<td>up</td>
<td>up</td>
<td>3001:1::1234</td>
</tr>
</tbody>
</table>

*down: administratively down

Switch# show ipv6 interface eth-0-1 brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>Status</th>
<th>Protocol</th>
<th>IPv6 address</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-0-1</td>
<td>up</td>
<td>up</td>
<td>3001:1::1234</td>
</tr>
</tbody>
</table>

**Related Commands**

ipv6 enable
ipv6 address

7.3.7  **ipv6 verify unicast reverse-path**

**Command Purpose**

Use this command to enable urpf (unicast reverse path forwarding) on the interface. Use the no form of this command to disable urpf on the interface.

**Command Syntax**

ipv6 verify unicast reverse-path
no ipv6 verify unicast reverse-path

**Command Mode**

Interface Configuration

**Default**

Urpf is disabling on the interface by default.

**Usage**

Use this command to enable urpf (unicast reverse path forwarding) on the interface. Use the no form of this command to disable urpf on the interface.

**Examples**

The following example shows how to enable URPF for IPv6:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 verify unicast reverse-path
**Related Commands**

show ipv6 interface

### 7.3.8 ipv6 icmp error-interval

**Command Purpose**

Use this command to set the ipv6 icmp error-interval. Use the no form of this command to set the ipv6 icmp error-interval to default.

**Command Syntax**

```plaintext
no ipv6 icmp error-interval ERROR_INTERVAL
no ipv6 icmp error-interval
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>error-interval</td>
<td>ICMPv6 Error message interval.</td>
<td>0–2147483647 ms</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

1000 milliseconds.

**Usage**

None

**Examples**

The following example shows how to set the ICMPv6 error interval:

```plaintext
Switch# configure terminal
Switch(config)# ipv6 icmp error-interval 2000
```

**Related Commands**

None

### 7.3.9 clear ipv6 route static

**Command Purpose**

Use this command to clear static ipv6 routes.

**Command Syntax**

```plaintext
clear ipv6 route static
```

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

The following example shows how to clear ipv6 static routes:

```plaintext
Switch# clear ipv6 route static
```

**Related Commands**

None
7.4 Ipv6 Prefix-list Commands

7.4.1 ipv6 prefix-list

Command Purpose
To create a ipv6 prefix list or add a prefix-list entry, use the ipv6 prefix-list command in global configuration mode.
To delete a prefix-list or an entry, use the no form of this command.

Command Syntax
ipv6 prefix-list WORD [ seq SEQUENCE-NUMBER ] [ deny ] [ permit ] [ any ] [ IPv6-ADDRESS /M [ ge GE-LENGTH ] [ le LE-LENGTH ] ]
no ipv6 prefix-list WORD [ seq SEQUENCE-NUMBER ] [ deny ] [ permit ] [ any ] [ IPv6-ADDRESS /M [ ge GE-LENGTH ] [ le LE-LENGTH ] ]
no ipv6 prefix-list WORD

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>Config a name to identify the prefix list</td>
<td>Up to 40 characters</td>
</tr>
<tr>
<td>seq SEQUENCE-NUMBER</td>
<td>Applies a sequence number to a prefix-list entry. The range of sequence number that can be entered is from 1 to 65535. If a sequence number is not entered when configuring this command, a default sequence numbering is applied to the prefix list. The number 5 is applied to the first prefix entry, and subsequent unnumbered entries are incremented by 5.</td>
<td>1-65535</td>
</tr>
<tr>
<td>deny</td>
<td>Denies access for a matching condition</td>
<td>-</td>
</tr>
<tr>
<td>permit</td>
<td>Permits access for a matching condition</td>
<td>-</td>
</tr>
<tr>
<td>IPv6-ADDRESS /M</td>
<td>Configures the network address, and the length of the network mask in bits. The network number can be any valid IPv6 address or prefix. The bit mask can be a number from 0 to 128.</td>
<td>IPv6 address and mask length between 1-128</td>
</tr>
<tr>
<td>ge GE-LENGTH</td>
<td>(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.</td>
<td>1-128</td>
</tr>
<tr>
<td>le LE-LENGTH</td>
<td>(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.</td>
<td>1-128</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
No prefix lists are created.

Usage
The ipv6 prefix-list command is used to configure IPv6 prefix filtering. Prefix lists are configured with permit or deny keywords to either permit or deny the prefix based on the matching condition. A prefix list consists of an IPv6 address and a bit mask. The IPv6 address can be global address, or a link-local address. The bit mask is entered as a number from 1 to 128. An implicit deny is applied to traffic that does not match any prefix-list entry. Prefix lists are configured to match an exact prefix length or a prefix range. The ge and le keywords are used to specify a range of the prefix lengths to match, providing more flexible configuration than can be configured with just the network/length argument. The prefix list is processed using an exact match when neither the ge nor le keyword is entered. If only the ge value is entered, the range is the value entered for the ge ge-length argument to a full 128-bit length. If only the le value is entered, the range is from value entered for the network/length argument to the le le-length argument. If both the ge ge-length and le le-length...
keywords and arguments are entered, the range falls between the values used for the ge-length and le-length arguments. The following formula shows this behavior:

\[
\text{network/length} < \text{ge ge-length} \leq \text{le-le-length} \leq 128 .
\]

A prefix list is configured with a name and/or sequence number. One or the other must be entered when configuring this command. If a sequence number is not entered, a default sequence number of 5 is applied to the prefix list. And subsequent prefix list entries will be incremented by 5 (for example, 5, 10, 15, and onwards). If a sequence number is entered for the first prefix list entry but not subsequent entries, then the subsequent entries will also be incremented by 5 (for example, if the first configured sequence number is 3, then subsequent entries will be 8, 13, 18, and onwards). Default sequence numbers can be suppressed by entering the no form of this command with the seq keyword. Prefix lists are evaluated starting with the lowest sequence number and continues down the list until a match is made. Once a match is made that covers the network the permit or deny statement is applied to that network and the rest of the list is not evaluated.

**Examples**

The following example shows how to configure ipv6 prefix-list: To deny the default route ::/0:

```bash
Switch# configure terminal
Switch(config)# ipv6 prefix-list abc deny ::/0
```

To permit the prefix 2001:db8::/64:

```bash
Switch# configure terminal
Switch(config)# ipv6 prefix-list abc permit 2001:db8::/64
```

To accept a mask length of up to 64 bits in routes with the prefix 2001:db8::/32:

```bash
Switch# configure terminal
Switch(config)# ipv6 prefix-list abc permit 2001:db8::/32 le 64
```

To deny mask lengths greater than 64 bits in routes with the prefix 2001:db8::/32:

```bash
Switch# configure terminal
Switch(config)# ipv6 prefix-list abc deny 2001:db8::/32 ge 64
```

**Related Commands**

- `ipv6 prefix-list description`  
- `ipv6 prefix-list sequence`  
- `show ipv6 prefix-list`  
- `clear ipv6 prefix-list`

### 7.4.2 ipv6 prefix-list description

**Command Purpose**

To add a text description of a ipv6 prefix list, use the ipv6 prefix-list description command in global configuration mode. To remove the text description, use the no form of this command.

**Command Syntax**

```
ipv6 prefix-list WORD description LINE  
no ipv6 prefix-list WORD description [ LINE ]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>Name of prefix list</td>
<td>Up to 40 characters</td>
</tr>
<tr>
<td>LINE</td>
<td>The description of this prefix-list</td>
<td>Up to 80 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

There is no description for prefix-list.

**Usage**

The ipv6 prefix list will be created if it didn't exist.

**Examples**

The following example shows how to add description:

```bash
Switch# configure terminal
Switch(config)# ipv6 prefix-list abc description Permit routes from customer A
```
Related Commands
ipv6 prefix-list
ipv6 prefix-list sequence
show ipv6 prefix-list
clear ipv6 prefix-list

7.4.3 ipv6 prefix-list sequence-number

Command Purpose
To enable the generation of sequence numbers for entries in a ipv6 prefix list, use the ipv6 prefix-list sequence-number command in global configuration mode. To disable this function, use the no form of this command.

Command Syntax
ipv6 prefix-list sequence-number
no ipv6 prefix-list sequence-number

Command Mode
Global Configuration

Default
This command has no default behavior.

Usage
This command is used to enable sequence-number display.

Examples
The following example shows how to enable ipv6 prefix-list sequence-number:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 prefix-list sequence-number

Related Commands
ipv6 prefix-list
show ipv6 prefix-list
clear ipv6 prefix-list

7.4.4 show ipv6 prefix-list

Command Purpose
To show ipv6 prefix list information, use the show ipv6 prefix-list command.

Command Syntax
show ipv6 prefix-list { summary | detail } ( WORD | )
show ipv6 prefix-list WORD { seq SEQUENCE-NUMBER | IPv6-ADDRESS /M ( longer | first-match ) | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>Summary of prefix lists</td>
<td>-</td>
</tr>
<tr>
<td>detail</td>
<td>Detail of prefix lists</td>
<td>-</td>
</tr>
<tr>
<td>WORD</td>
<td>Name of the prefix list</td>
<td>Up to 40 characters</td>
</tr>
<tr>
<td>seq SEQUENCE-NUMBER</td>
<td>sequence number of the entry in the ipv6 prefix list</td>
<td>1-65535</td>
</tr>
<tr>
<td>IPv6-ADDRESS /M</td>
<td>IPv6 prefix &lt;network&gt;/&lt;length&gt;, e.g., 2001:db8::/32</td>
<td>IPv6 address and mask length between 1-128</td>
</tr>
<tr>
<td>longer</td>
<td>Lookup longer prefix</td>
<td>-</td>
</tr>
<tr>
<td>first-match</td>
<td>First matched prefix</td>
<td>-</td>
</tr>
</tbody>
</table>
Command Mode
Privileged EXEC

Default
This command has no default behavior.

Usage
None

Examples
The following example shows how to display ip prefix-list:
Switch# show ipv6 prefix-list
ipv6 prefix-list ripng_pre: 5 entries
  seq 1 deny 2001:db8:9::/64
  seq 2 deny 2001:db8:10::/64
  seq 3 deny 2001:db8:11::/64
  seq 4 deny 2001:db8:12::/64
  seq 5 permit any

Related Commands
ipv6 prefix-list
clear ipv6 prefix-list

7.4.5 clear ipv6 prefix-list

Command Purpose
To reset the hit count of the prefix list entries, use the clear ipv6 prefix-list command.

Command Syntax
clear ipv6 prefix-list { WORD ( IPv6-ADDRESS /M ) } |

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>Name of the prefix list</td>
<td>Up to 40 characters</td>
</tr>
<tr>
<td>IPv6-ADDRESS /M</td>
<td>IPv6 prefix &lt;network&gt;/&lt;length&gt;, e.g., 2001:db8::32</td>
<td>IPv6 address and mask length between 1-128</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
This command has no default behavior.

Usage
None

Examples
The following example shows how to clear ipv6 prefix-list:
Switch(config)# clear ipv6 prefix-list test

Related Commands
ipv6 prefix-list
7.5 Route Map Commands

7.5.1 route-map

Command Purpose
To define the conditions for redistributing routes from one routing protocol into another, or to enable policy routing in bgp, use the route-map command in global configuration mode and the match and set command in route-map configuration modes. To delete an entry, use the no form of this command.

Command Syntax

```
route-map MAP-TAG [ permit | deny ] [ sequence-NUMBER ]
no route-map MAP-TAG [ permit | deny ] [ SEQUENCE_NUMBER ]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAP-TAG</td>
<td>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.</td>
<td>The length of route-map name should not greater than 20 and the first character should be 'a'-'z','A'-'Z' or '0'-'9'.</td>
</tr>
<tr>
<td>permit</td>
<td>(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.</td>
<td>-</td>
</tr>
<tr>
<td>deny</td>
<td>(Optional) If the match criteria are met for the route map and the deny keyword is specified, the route is not redistributed</td>
<td>-</td>
</tr>
<tr>
<td>SEQUENCE_NUMBER</td>
<td>(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</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

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

7.5.2 match as-path

Command Purpose

Use this command to match an autonomous system path access list.
Use the no parameter with this command to remove a path list entry.
The match as-path command specifies the autonomous system path to be matched. If there is a match for the specified AS path, and
permit is specified, the route is redistributed or controlled, as specified by the set action. If the match criteria are met, and deny is specified,
the route is not redistributed or controlled. If the match criteria are not met then the route is neither accepted nor forwarded, irrespective
of permit or deny specifications.
The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take
different routes, depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding
specified in routing tables.

Command Syntax

match as-path LISTNAME
no match as-path

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISTNAME</td>
<td>Specifies as autonomous system path access list name</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode

Route-map Configuration

Default

No match as-path is specified by default.

Usage

This command is valid only for BGP.

Examples

Switch# configure terminal
Switch(config)# route-map myroute deny 34
Switch(config-route-map)# match as-path myaccesslist
Related Commands

match metric
match ip address
match community
set as-path
set community

7.5.3 match community

Command Purpose
Use this command to specify the community to be matched.
Use the no parameter with this command to remove the community list entry.
Communities are used to group and filter routes. They are designed to provide the ability to apply policies to large numbers of routes by using match and set commands. Community lists are used to identify and filter routes by their common attributes.
Use the match community command to allow matching based on community lists.
The values set by the match community command overrides the global values. The route that does not match at least one match clause is ignored.

Command Syntax

match community WORD
no match community

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>Specifies the Community-list name</td>
<td>Up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode
Route-map Configuration

Default
No match community is specified by default.

Usage
This command is valid only for BGP.

Examples

Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# match community mylist

Related Commands

match ip address
match as-path
set as-path
set community
match metric

7.5.4 match interface

Command Purpose
Use this command to define the interface match criterion.
Use the no parameter with this command to remove the specified match criterion.
The match interface command specifies the next-hop interface name of a route to be matched.

Command Syntax

match interface IFNAME
no match interface
### Command Mode

Route-map Configuration

### Default

No match interface is specified by default.

### Usage

None

### Examples

Switch# configure terminal
Switch(config)# route-map mymap1 permit 10
Switch(config-route-map)# match interface eth-0-1

### Related Commands

match tag
match route-type external

#### 7.5.5 match ipv6 address

**Command Purpose**

Use this command to specify the match address of route.

Use the no parameter with this command to remove the match ipv6 address entry.

The match ipv6 address command specifies the IPv6 address to be matched. If there is a match for the specified IPv6 address, and permit is specified, the route is redistributed or controlled, as specified by the set action. If the match criteria are met, and deny is specified then the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of permit or deny specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes, depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

**Command Syntax**

match ipv6 address ACCESSSLISTID
no match ipv6 address

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCESSSLISTID</td>
<td>Specify a IPv6 access-list name, up to 20 characters</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Route-map Configuration

**Default**

No match ipv6 address is specified by default.

**Usage**

This command is valid for BGP, OSPFv3 and RIPng only.

**Examples**

Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# match ipv6 address List1
Related Commands
match community
match as-path
set as-path
set community
match metric

7.5.6  match ipv6 address prefix-list

Command Purpose
Use this command to match entries of ipv6 prefix-lists.
Use the no parameter with this command to disable this function
This command specifies the entries of prefix-lists to be matched. If there is a match for the specified ipv6 prefix-list entries, and permit is specified, the route is redistributed or controlled, as specified by the set action. If the match criteria are met, and deny is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of permit or deny specifications.
The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Command Syntax
match ipv6 address prefix-list LISTNAME
no match ipv6 address prefix-list (LISTNAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISTNAME</td>
<td>Specifies the IPv6 prefix list name</td>
<td>Up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode
Route-map Configuration

Default
No match ipv6 address prefix-list is specified by default.

Usage
This command is valid for BGP, OSPFv3 and RIPng only.

Examples
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)#match ipv6 address prefix-list mylist

Related Commands
match community
match as-path
set as-path
set community
match metric

7.5.7  match ipv6 next-hop

Command Purpose
Use this command to specify a ipv6 next-hop address to be matched in a route-map.
Use the no parameter with this command to disable this function.
The match ipv6 next-hop command specifies the next-hop address to be matched. If there is a match for the specified next-hop address, and permit is specified, the route is redistributed or controlled as specified by the set action. If the match criteria are met, and deny is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of permit or deny specifications.
The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

**Command Syntax**

```plaintext
match ipv6 next-hop ( IPV6_ADDR | ACCESSSLISTID )
no match ipv6 next-hop [ IPV6-ADDRESS | ACCESSSLISTID ]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPV6_ADDR</td>
<td>Specify a IPv6 address, e.g., 2001:db8:1</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>ACCESSSLISTID</td>
<td>Specify a IPv6 access-list name</td>
<td>up to 20 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Route-map Configuration

**Default**

No match ipv6 next-hop is specified by default.

**Usage**

This command is valid for BGP, OSPFv3 and RIPng only.

**Examples**

Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# match ipv6 next-hop mylist

**Related Commands**

- match community
- match as-path
- set as-path
- set community
- match metric

7.5.8  match ipv6 next-hop prefix-list

**Command Purpose**

Use this command to specify the next-hop IPv6 address match criterion, using the prefix-list. Use the no parameter with this command to remove the specified match criterion. Use the match ipv6 next-hop prefix-list command to match the next-hop IPv6 address of a route.

**Command Syntax**

```plaintext
match ipv6 next-hop prefix-list LISTNAME
no match ipv6 next-hop prefix-list [ LISTNAME ]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISTNAME</td>
<td>A string specifying the ipv6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>prefix-list name</td>
<td></td>
</tr>
</tbody>
</table>

**Command Mode**

Route-map Configuration

**Default**

No match ipv6 next-hop prefix-list is specified by default.

**Usage**

This command is valid for RIPng only.
Examples

Switch# configure terminal
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# match ipv6 next-hop prefix-list list1

Related Commands

match metric
match interface
match ip next-hop

7.5.9 match local-preference

Command Purpose

Use this command to specify the local-preference match criterion.
Use the no parameter with this command to remove the specified match criterion.
Use the match local-preference command to match the local preference of a route.

Command Syntax

match local-preference LOCAL-PREFERENCE
no match local-preference

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOCAL-PREFERENCE</td>
<td>Species the preference value</td>
<td>0-4294967295</td>
</tr>
</tbody>
</table>

Command Mode

Route-map Configuration

Default

No match local-preference is specified by default.

Usage

This command is valid for BGP only.

Examples

Switch# configure terminal
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# match local-preference 100

Related Commands

match community
match as-path
set as-path
set community
match ip next-hop

7.5.10 match metric

Command Purpose

Use this command to match a metric of a route.
Use the no parameter with this command to disable this function.
The match metric command specifies the metric to be matched. If there is a match for the specified metric, and permit is specified, the route is redistributed or controlled as specified by the set action. If the match criteria are met, and deny is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of permit or deny specifications.
The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.
Command Syntax

match metric METRICVAL
no match metric

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>METRICVAL</td>
<td>metric value</td>
<td>0-4294967295</td>
</tr>
</tbody>
</table>

Command Mode

Route-map Configuration

Default

No match metric is specified by default.

Usage

This command is valid for BGP, OSPF and RIP only.

Examples

Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# no match metric

Related Commands

match community
match as-path
set as-path
set community
match ip next-hop

7.5.11 match origin

Command Purpose

Use this command to match origin code.

Use the no parameter with this command to disable this matching.

The origin attribute defines the origin of the path information. The egp parameter is indicated as an e in the routing table, and it indicates that the origin of the information is learned via Exterior Gateway Protocol. The igp parameter is indicated as an i in the routing table, and it indicates the origin of the path information is interior to the originating AS.

The incomplete parameter is indicated as a ? in the routing table, and indicates that the origin of the path information is unknown or learned through other means. If a static route is redistributed into BGP, the origin of the route is incomplete.

The match origin command specifies the origin to be matched. If there is a match for the specified origin, and permit is specified, the route is redistributed or controlled as specified by the set action. If the match criteria are met, and deny is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of permit or deny specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Command Syntax

match origin (egp | igp | incomplete)
no match origin

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>egp</td>
<td>learned from EGP</td>
<td>-</td>
</tr>
<tr>
<td>igp</td>
<td>Local IGP</td>
<td>-</td>
</tr>
<tr>
<td>incomplete</td>
<td>Unknown heritage</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Route-map Configuration
Default

No match origin is specified by default.

Usage

None

Examples

Switch# configure terminal
Switch(config)# route-map myroute deny 34
Switch(config-route-map)# match origin egp

Related Commands

None

7.5.12 match route-type

Command Purpose

Use this command to match specified external route type.
Use the no parameter with this command to turn off the matching.
Use the match route-type external command to match specific external route types. AS-external LSA is either Type-1 or Type-2. External type-1 matches only Type 1 external routes, and external type-2 matches only Type 2 external routes.

Command Syntax

match route-type external { type-1 | type-2 }
no match route-type external

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>type-1</td>
<td>Match OSPF External Type 1 metrics</td>
<td>-</td>
</tr>
<tr>
<td>type-2</td>
<td>Match OSPF External Type 1 metrics</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Route-map Configuration

Default

No match route-type is specified by default.

Usage

This command is valid for OSPF only

Examples

Switch# configure terminal
Switch(config)# route-map mymap1 permit 10
Switch(config-route-map)# match route-type external type-1

Related Commands

match tag

7.5.13 match tag

Command Purpose

Use this command to match the specified tag value.
Use the no parameter with this command to turn off the declaration.
Use the match tag command to match the specified tag value.
Command Syntax

match tag TAG
no match tag

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TAG</td>
<td>Specifies the tag value</td>
<td>0-4294967295</td>
</tr>
</tbody>
</table>

Command Mode

Route-map Configuration

Default

No match tag is specified by default.

Usage

This command is valid for OSPF RIP only.

Examples

Switch# configure terminal
Switch(config)# route-map mymap1 permit 10
Switch(config-route-map)# match tag 100

Related Commands

match metric
match route-type external

7.5.14 set ipv6 aggregator

Command Purpose

Use this command to set the AS number for the route map and router ID.
Use the no parameter with this command to disable this function.
An Autonomous System (AS) is a collection of networks under a common administration sharing a common routing strategy. It is subdivided by areas, and is assigned a unique 16-bit number. Use the set aggregator command to assign an AS number for the aggregator.
To use the set aggregator command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.
If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax

set ipv6 aggregator as ASNUM IPV6_ADDR
no set ipv6 aggregator

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASNUM</td>
<td>Specifies the AS number of aggregator</td>
<td>1-65535</td>
</tr>
<tr>
<td>IPV6_ADDR</td>
<td>Specifies the IPv6 address of aggregator</td>
<td>IPv6 Address</td>
</tr>
</tbody>
</table>

Command Mode

Route-map Configuration

Default

No set aggregator is specified by default.

Usage

This command is valid for BGP only.
Examples
Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# set aggregator as 43 2001:db8::1

Related Commands
None

7.5.15 set as-path

Command Purpose
Use this command to modify an autonomous system path for a route.
Use the no parameter with this command to disable this function.
Use the set as-path command to specify an autonomous system path. By specifying the length of the AS-Path, the router influences the best path selection by a neighbor. Use the prepend parameter with this command to prepend an AS path string to routes increasing the AS path length.
To use the set as-path command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.
If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax
set as-path prepend ASN [ ... ASN ]
no set as-path

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASN</td>
<td>System prepends this number to the AS path</td>
<td>1-4294967295</td>
</tr>
<tr>
<td>prepend</td>
<td>Prepends the autonomous system path</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Route-map Configuration

Default
No set as-path is specified by default.

Usage
This command is valid for BGP only.

Examples
Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# set as-path prepend 8 24

Related Commands
None

7.5.16 set atomic-aggregate

Command Purpose
Use this command to set an atomic aggregate attribute.
Use the no parameter with this command to disable this function.
To use the set atomic aggregate command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.
If the packets do not match any of the defined criteria, they are routed through the normal routing process.
Command Syntax

set atomic-aggregate
no set atomic-aggregate

Command Mode

Route-map Configuration

Default

No set atomic-aggregate is specified by default.

Usage

This command is valid for BGP only.

Examples

Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set atomic-aggregate

Related Commands

None

7.5.17 set comm-list delete

Command Purpose

Use this command to delete the matched communities from the community attribute of an inbound or outbound update when applying route-map.
Use the no parameter with this command to disable this feature.

Command Syntax

set comm-list { STANDARD | EXPANDED | WORD } delete
no set comm-list

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>STANDARD</td>
<td>Standard community-list number</td>
<td>1-99</td>
</tr>
<tr>
<td>EXPANDED</td>
<td>Expanded community-list number</td>
<td>100-199</td>
</tr>
<tr>
<td>WORD</td>
<td>Name of the Community-list</td>
<td>up to 255 characters</td>
</tr>
<tr>
<td>delete</td>
<td>Delete matching communities</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Route-map Configuration

Default

No set comm-list is specified by default.

Usage

This command is valid for BGP only.

Examples

Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set comm-list 34 delete

Related Commands

None
7.5.18 set community

Command Purpose

Use this command to set the communities attribute.
Use the no parameter with this command to delete the entry.
Use this command to set the community attribute and group destinations in a certain community, as well as, apply routing decisions according to those communities.
To use the set community command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met. If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax

set community [ AA:NN | internet | local-AS | no-advertise | no-export ]
set community none
no set community

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA:NN</td>
<td>AA:NN: Specifies the community number in this format</td>
<td>Support 2 bytes AS number and 4 bytes community ID</td>
</tr>
<tr>
<td></td>
<td>AA = The AS number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NN = The number assigned to community</td>
<td></td>
</tr>
<tr>
<td>internet</td>
<td>Specifies the Internet (well-known community)</td>
<td>-</td>
</tr>
<tr>
<td>local-AS</td>
<td>Specifies no sending outside the local AS (well-known community)</td>
<td>-</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Specifies no advertisement of this route to any peer</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>(well-known community)</td>
<td></td>
</tr>
<tr>
<td>no-export</td>
<td>Specifies no advertisement of this route to next AS</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>(well-known community)</td>
<td></td>
</tr>
<tr>
<td>none</td>
<td>Removes the community attribute from the prefixes that pass the route-map</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Route-map Configuration

Default

No set community is specified by default.

Usage

This command is valid for BGP only.

Examples

The following examples show the use of the set community command with different parameters:

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set community no-export no-advertise
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set community no-advertise
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set community 10:01 23:34 12:14 no-export
```

Related Commands

None
7.5.19 set dampening

**Command Purpose**

Use this command to enable route-flap dampening and set parameters. Use the no parameter with this command to disable it. Set the unreachable 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 Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>REACHTIME</strong></td>
<td>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</td>
<td>1-45</td>
</tr>
<tr>
<td><strong>REUSE</strong></td>
<td>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</td>
<td>1-20000</td>
</tr>
<tr>
<td><strong>SUPPRESS</strong></td>
<td>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</td>
<td>1-20000</td>
</tr>
<tr>
<td><strong>MAXSUPPRESS</strong></td>
<td>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)</td>
<td>1-255</td>
</tr>
<tr>
<td><strong>UNREACHTIME</strong></td>
<td>Specifies the un-reachability half-life time for penalty, in minutes. The default value is 15 minutes</td>
<td>1-45</td>
</tr>
</tbody>
</table>

**Command Mode**

Route-map Configuration

**Default**

Reference to the syntax description above.

**Usage**

This command is valid for BGP only.

**Examples**

Switch# configure terminal
Switch(config)# route-map R1 permit 24
Switch(config-route-map)# set dampening 20 333 534 30

**Related Commands**

None

7.5.20 set extcommunity

**Command Purpose**

Use this command to set an extended community attribute. Use the no parameter with this command to disable this function.
To use the set extcommunity command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met. If the packets do not match any of the defined criteria, they are routed through the normal routing process.

**Command Syntax**

```
set extcommunity { rt | soo } EXTCOMMNUMBER [ … EXTCOMMNUMBER ]
no set extcommunity { rt | soo }
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>rt</td>
<td>Specifies the route target of the extended community</td>
<td>-</td>
</tr>
<tr>
<td>soo</td>
<td>Specifies the site-of-origin of the extended community</td>
<td>-</td>
</tr>
<tr>
<td>EXTCOMMNUMBER</td>
<td>ASN:NN_or_IP-address:nn VPN extended community</td>
<td>-</td>
</tr>
<tr>
<td>ASN:NN</td>
<td>the AS number</td>
<td>Support 2 bytes AS number and 4 bytes community ID</td>
</tr>
<tr>
<td>IPAddress</td>
<td>the AS number in IP address form</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

**Command Mode**

Route-map Configuration

**Default**

No set extcommunity is specified by default.

**Usage**

This command is valid for BGP only.

**Examples**

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set extcommunity rt 06:01
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set extcommunity rt 0.0.0.6:01
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set extcommunity soo 06:01
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set extcommunity soo 0.0.0.6:01
```

**Related Commands**

None

**7.5.21 set ipv6 next-hop**

**Command Purpose**

Use this command to set the specified next-hop ipv6 address value. Use the no parameter with this command to turn off the setting. Use this command to set the next-hop IPv6 address to the routes.

**Command Syntax**

```
set ipv6 next-hop [ local ] IPV6_ADDR
no set ipv6 next-hop [ local ]
```
### Command Mode
**Route-map Configuration**

### Default
No set ipv6 next-hop is specified by default.

### Usage
This command is valid for BGP, OSPFv3, and RIPng only.

### Examples
```
Switch# configure terminal
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# set ipv6 next-hop 2001:db8::1
```

### Related Commands
None

### 7.5.22 set local-preference

#### Command Purpose
Use this command to set the specified local-preference value.
Use the no parameter with this command to turn off the setting.
Use this command to set the local-preference value of the routes

#### Command Syntax
```
set local-preference LOCAL-PREFERENCE
no set local-preference
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOCAL-PREFERENCE</td>
<td>Species the preference value</td>
<td>0-4294967295</td>
</tr>
</tbody>
</table>

#### Command Mode
**Route-map Configuration**

#### Default
No set local-preference is specified by default.

#### Usage
This command is valid for BGP only.

#### Examples
```
Switch# configure terminal
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# set local-preference 100
```

#### Related Commands
None
7.5.23 set metric

Command Purpose

Use this command to set a metric value for a route.
Use the no parameter with this command to disable this function.
This command sets the metric value for a route, and influences external neighbors about the preferred path into an Autonomous System (AS). The preferred path is the one with a lower metric value. A router compares metrics for paths from neighbors in the same ASs. To compare metrics from neighbors coming from different ASs, use the bgp always-compare-med command.
To use the set metric command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.
If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax

set metric METRICVAL
no set metric

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>METRICVAL</td>
<td>metric value</td>
<td>0-4294967295</td>
</tr>
</tbody>
</table>

Command Mode

Route-map Configuration

Default

No set metric is specified by default.

Usage

This command is valid for BGP, OSPF and RIP.

Examples

Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set metric 600

Related Commands

None

7.5.24 set metric-type

Command Purpose

Use this command to set the metric type for the destination routing protocol.
Use the no parameter with this command to return to the default.
This command sets the type to either Type-1 or Type-2 in the AS-external-LSA when the route-map matches the condition.

Command Syntax

set metric-type { TYPE1 | TYPE2 }
no set metric-type

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>type1</td>
<td>Select to set external type 1 metric</td>
<td>-</td>
</tr>
<tr>
<td>type2</td>
<td>Select to set external type 2 metric</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Route-map Configuration
Default

No set metric-type is specified by default.

Usage

This command is valid for OSPF only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set metric-type 1
```

Related Commands

None

7.5.25 set origin

Command Purpose

Use this command to set the BGP origin code.
Use the no parameter with this command to delete an entry.
The origin attribute defines the origin of the path information. The three parameters with this command indicate three different values. IGP is interior to the originating AS. This happens if IGP is redistributed into the BGP. EGP is learned through an Exterior Gateway Protocol. Incomplete is unknown or learned through some other means. This happens when static route is redistributed in BGP and the origin of the route is incomplete.
To use the set origin command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met. If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax

```
set origin { egp | igp | incomplete }
no set origin
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>egp</td>
<td>Specifies a remote EGP system</td>
<td>-</td>
</tr>
<tr>
<td>igp</td>
<td>A local IGP system</td>
<td>-</td>
</tr>
<tr>
<td>incomplete</td>
<td>Specifies a system of unknown heritage</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Route-map Configuration

Default

No set origin is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set origin egp
```

Related Commands

None
7.5.26 set ipv6 originator-id

Command Purpose
Use this command to set the originator ID attribute. Use the no parameter with this command to disable this function.
To use the set originator-id command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.
If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax
set ipv6 originator-id IPV6_ADDR
no set ipv6 originator-id

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPV6_ADDR</td>
<td>Specifies the IPv6 address</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td></td>
<td>of originator</td>
<td></td>
</tr>
</tbody>
</table>

Command Mode
Route-map Configuration

Default
No set originator-id is specified by default.

Usage
This command is valid for BGP only.

Examples
$Switch# configure terminal
$Switch(config)# route-map rmap1 permit 3
$Switch(config-route-map)# set ipv6 originator-id 2001:db8::1

Related Commands
None

7.5.27 set tag

Command Purpose
Use this command to set a specified tag value. Use the no parameter with this command to return to the default.
Tag in this command is the route tag which is labeled by another routing protocol (BGP or other IGP when redistributing), because AS-external-LSA has a route-tag field in its LSAs. Also, with using route-map, ZebOS can tag the LSAs with the appropriate tag value. Sometimes, the tag matches with using route-map, and sometimes, the value may be used by another application.

Command Syntax
set tag TAGVALUE
no set tag

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TAGVALUE</td>
<td>Tag value for destination</td>
<td>0-4294967295</td>
</tr>
<tr>
<td></td>
<td>routing protocol.</td>
<td></td>
</tr>
</tbody>
</table>

Command Mode
Route-map Configuration

Default
No set tag is specified by default.
Usage

This command is valid for OSPF and RIP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set tag 6
```

Related Commands

redistribute
default-information

7.5.28 set vpnv6 next-hop

Command Purpose

Use this command to set a VPNv6 next-hop address.
Use the no parameter with this command to disable this function.

To use the set vpnv6-next-hop command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax

```
set vpnv6 next-hop IPV6_ADDR
no set vpnv6 next-hop
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPV6_ADDR</td>
<td>Specifies the IPv6 address of originator</td>
<td>IPv6 Address</td>
</tr>
</tbody>
</table>

Command Mode

Route-map Configuration

Default

No set vpnv6 next-hop is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set vpnv6 next-hop 2001:db8::1
```

Related Commands

None

7.5.29 set weight

Command Purpose

Use this command to set weights for the routing table.
Use the no parameter with this command to delete an entry.

The weight value is used to assist in best path selection. It is assigned locally to a router. When there are several routes with a common destination, the routes with a higher weight value are preferred.

To use the set weight command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.

match as-path 10
set weight 400
In the above configuration, all routes that apply to access-list 10 will have the weight set at 400. If the packets do not match any of the defined criteria, they are routed through the normal routing process.

**Command Syntax**

set weight *WEIGHT*
no set weight

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEIGHT</td>
<td>Specifies the weight value</td>
<td>0-4294967295</td>
</tr>
</tbody>
</table>

**Command Mode**

Route-map Configuration

**Default**

No set weight is specified by default.

**Usage**

This command is valid for BGP only.

**Examples**

Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set weight 60

**Related Commands**

match as-path

7.5.30 show route-map

**Command Purpose**

Use this command to display user readable route-map information.

**Command Syntax**

show route-map [ NAME ]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>route-map name</td>
<td>The length of route-map name should not greater than 20 and the first character should be 'a'-'z', 'A'-'Z' or '0'-'9'.</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

Switch1# show route-map
route-map abc, permit, sequence 10
  Match clauses:
    ip address acl1

www.fs.com
### 7.6 IPv6 BGP Commands

#### 7.6.1 address-family

**Command Purpose**

Use this command to enter the IPv6 address-family command mode.

**Command Syntax**

```
address-family ipv6 ( unicast | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>unicast</td>
<td>Specifies unicast prefixes.</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration

**Default**

None

**Usage**

Use the address family command to enter the address family mode allowing configuration of address-family specific parameters. To leave the address family mode and return to the Configure mode use the exit-address-family command.

**Examples**

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router)address-family ipv6
```

**Related Commands**

exit-address-family

#### 7.6.2 aggregate-address

**Command Purpose**

Use this command to configure BGP aggregate entries. Use the no parameter with this command to disable this function.

**Command Syntax**

```
( no ) aggregate-address IPv6_ADDR { summary-only | as-set }
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPV6_ADDR</td>
<td>X::X::X/M Specifies the aggregate prefix</td>
<td>IPv6 address</td>
</tr>
<tr>
<td>summary-only</td>
<td>Filters more specific routes from updates.</td>
<td>-</td>
</tr>
<tr>
<td>as-set</td>
<td>Generates AS set path information</td>
<td>-</td>
</tr>
</tbody>
</table>
Command Mode
Address Family Configuration

Default
Disabled

Usage
Aggregates are used to minimize the size of routing tables. Aggregation combines the characteristics of several different routes and advertises a single route. The aggregate-address command creates an aggregate entry in the BGP routing table if any more-specific BGP routes are available in the specified range. Using the summary-only parameter advertises the prefix only, suppressing the more-specific routes to all neighbors.

Examples
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# aggregate-address 2018::1/64 as-set summary-only

Related Commands
N/A

7.6.3 bgp always-compare-med

Command Purpose
Use this command to compare the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems. Use the no parameter with this command to disallow the comparison.

Command Syntax
( no ) bgp always-compare-med

Command Mode
Router Configuration

Default
Disabled

Usage
Multi Exit Discriminator (MED) is used in best path selection by BGP. MED is compared after BGP attributes weight, local preference, AS-path and origin have been compared and are equal. MED comparison is done only among paths from the same autonomous system (AS). Use bgp always-compare-med command to allow comparison of MEDs from different ASs. The MED parameter is used to select the best path. A path with lower MED is preferred.

Examples
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp always-compare-med

Related Commands
bgp bestpath med
t bestpath as-path ignore

7.6.4 bgp bestpath as-path ignore

Command Purpose
Use this command to prevent the router from considering as-path as a factor in the algorithm for choosing a route. Use the no parameter with this command to allow the router to consider as-path in choosing a route.
Command Syntax

(no) bgp bestpath as-path ignore

Command Mode

Router Configuration

Default

Disabled

Usage

None

Examples

Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp bestpath as-path ignore

Related Commands

bgp always-compare-med, bgp bestpath med, bgp bestpath compare-routerid

7.6.5 bgp bestpath compare-confed-aspath

Command Purpose

Use this command to allow comparing of the confederation AS path length.
Use the no parameter with this command to revert the selection and ignore AS confederation path length in the BGP best path selection.

Command Syntax

(no) bgp bestpath compare-confed-aspath

Command Mode

Router Configuration

Default

BGP receives routes with identical eBGP paths from eBGP peers and selects the first route received as the best path.

Usage

This command specifies that the AS confederation path length must be used, when available, in the BGP best path decision process. It is effective only when bgp bestpath as-path ignore command has not been specified.

Examples

Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp bestpath compare-confed-aspath

Related Commands

bgp bestpath as-path ignore

7.6.6 bgp bestpath compare-routerid

Command Purpose

Use this command to compare router-id for identical eBGP paths.
Use the no parameter with this command to disable this function.
Command Syntax

( no ) bgp bestpath compare-routerid

Command Mode

Router Configuration

Default

BGP receives routes with identical eBGP paths from eBGP peers and selects the first route received as the best path.

Usage

When comparing similar routes from peers the BGP router does not consider router ID of the routes. By default, it selects the first received route. Use this command to include router ID in the selection process; similar routes are compared and the route with lowest router ID is selected. The router-id is the highest IP address on the router, with preference given to loopback addresses. Router-id can be manually set by using the bgp router-id command.

Examples

Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp bestpath compare-routerid

Related Commands

show bgp ipv6
gshow ip bgp neighbors

7.6.7 bgp bestpath med

Command Purpose

Use this command to specify Multi Exit Discriminator (MED) attribute comparison.

Usage

Use the no parameter with this command to prevent BGP from considering the MED attribute in comparing paths.

Command Syntax

bgp bestpath med confed [ missing-as-worst ]
bgp bestpath med missing-as-worst [ confed ]
no bgp bestpath med confed [ missing-as-worst ]
no bgp bestpath med missing-as-worst [ confed ]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>confed</td>
<td>Compares MED among confederation paths</td>
<td>-</td>
</tr>
<tr>
<td>missing-as-worst</td>
<td>Treats missing MED as the least preferred one</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

MED value is zero.

Usage

Use this command to specify two MED attributes—confed and missing-as-worst. The confed attribute enables MED comparison among paths learned from confederation peers. The MEDs are compared only if there is no external autonomous system (an AS not within the confederation) in the path. If there is an external autonomous system in the path, the MED comparison is not made.

The missing-as-worst attribute to consider a missing MED attribute in a path as having a value of infinity, making the path without a MED value the least desirable path. If missing-as-worst is disabled, the missing MED is assigned the value of 0, making the path with the missing MED attribute the best path.
Examples

Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp bestpath med missing-as-worst

Related Commands

bgp-always-compare-med, bgp bestpath as-path ignore, bgp deterministic-med

7.6.8 bgp client-to-client reflection

Command Purpose

Use this command to restore route reflection from a BGP route reflector to clients. Use the no parameter with this command to turn off client-to-client reflection.

Command Syntax

bgp client-to-client reflection
no bgp client-to-client reflection

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>reflection</td>
<td>Allows reflection of routes</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

When a router is configured as a route reflector, client-to-client reflection is enabled by default.

Usage

The bgp client-to-client reflection command is used to configure routers as route reflectors. Route reflectors are used when all Interior Border Gateway Protocol (iBGP) speakers are not fully meshed. If the clients are fully meshed the route reflector is not required, use no bgp client-to-client reflection command to disable the client-to-client route reflection.

Examples

Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) no bgp client-to-client reflection

Related Commands

bgp cluster-id
neighbor route-reflector-client
show bgp ipv6

7.6.9 bgp cluster-id

Command Purpose

Use this command to configure the cluster ID if the BGP cluster has more than one route reflector. Use the no parameter with this command to remove the cluster ID.

Command Syntax

bgp cluster-id CLUSTERID
no bgp cluster-id
### 7.5.10 bgp cluster-id

**Parameter** | **Parameter Description** | **Parameter Value**
--- | --- | ---
CLUSTERID | A.B.C.D]<1-4294967295> Specifies the cluster ID of this router acting as a route reflector, either as IP address or as a maximum of 4 bytes. | IPv4 Address or Number between 1-4294967295
A.B.C.D | A.B.C.D Route Reflector Cluster-id in IP address format | IPv4 Address
<1-4294967295> | Route Reflector cluster-id as a 32 bit quantity | 1-4294967295

**Command Mode**

Router Configuration

**Default**

N/A

**Usage**

A cluster includes route reflectors and its clients. Usually, each cluster is identified by the router ID of its single route reflector but to increase redundancy sometimes a cluster may have more than one route reflector. All router reflectors in such a cluster are then identified by a cluster ID. The bgp cluster-id command is used to configure the 4 byte cluster ID for clusters with more than one route reflectors.

**Examples**

Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp cluster-id 1.1.1.1

**Related Commands**

bgp client-to-client reflection, neighbor route-reflector-client, show bgp ipv6

### 7.6.10 bgp confederation identifier

**Command Purpose**

Use this command to specify a Bgp confederation identifier. Use the no parameter with this command to remove the Bgp confederation identifier.

**Command Syntax**

bgp confederation identifier ID
no bgp confederation identifier

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Set routing domain confederation AS number</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration

**Default**

N/A

**Usage**

N/A

**Examples**

Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp confederation identifier 1
Related Commands

bgp confederation peer

7.6.11 bgp confederation peers

Command Purpose

Use this command to configure the Autonomous Systems (AS) that belong to the confederation. Use the no parameter with this command to remove an autonomous system from the confederation.

Command Syntax

bgp confederation peers .ASN
no bgp confederation peers (.ASN )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASN</td>
<td>AS numbers of eBGP peers that are under same confederation but in a different sub-AS</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

N/A

Usage

A confederation allows an AS to be divided into several ASs. The AS is given a confederation identifier. External routers view only the whole confederation as one AS. Each AS is fully meshed within itself and is visible internally to the confederation. Use the bgp confederation peer command to define the list of confederation peers.

Examples

Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp confederation peers 1234 21345

Related Commands

bgp confederation identifier

7.6.12 bgp dampening

Command Purpose

Use this command to set bgp dampening parameters. Use the no parameter with this command to unset the bgp dampening parameters.

Command Syntax

bgp dampening REACHTIME
bgp dampening REACHTIME REUSE
bgp dampening REACHTIME REUSE SUPPRESS MAXSUPPRESS ( UNREACHTIME )
bgp dampening route-map ROUTEMAP
no bgp dampening REACHTIME
no bgp dampening REACHTIME REUSE
no bgp dampening REACHTIME REUSE SUPPRESS MAXSUPPRESS ( UNREACHTIME )
no bgp dampening route-map ROUTEMAP
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>REACHTIME</td>
<td>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.</td>
<td>1-45</td>
</tr>
<tr>
<td>REUSE</td>
<td>Specifies the reuse limit value. When the penalty for a suppressed route decays below the reuse value, the routes become unsuppressed. The default reuse limit is 750 SUPPRESS &lt;1-20000&gt; 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.</td>
<td>1-20000</td>
</tr>
<tr>
<td>SUPPRESS</td>
<td>Specifies suppress-time. A route dampening more than this value will be suppressed. The default value is 2000.</td>
<td>1-20000</td>
</tr>
<tr>
<td>MAXSUPPRESS</td>
<td>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).</td>
<td>1-255</td>
</tr>
<tr>
<td>UNREACHTIME</td>
<td>Specifies the un-reachability half-life time for penalty, in minutes.</td>
<td>1-45</td>
</tr>
<tr>
<td>ROUTemap</td>
<td>route-map WORD Route-map to specify criteria for dampening.</td>
<td></td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration
Address Family Configuration

**Default**

N/A

**Usage**

Route dampening minimizes the instability caused by route flapping. A penalty is added for every flap in a flapping route. As soon as the total penalty reaches the suppress limit the advertisement of the route is suppressed. This penalty is decayed according to the configured half time value. Once the penalty is lower than the reuse limit, the route advertisement is un-suppressed. The dampening information is purged from the router once the penalty becomes less than half of the reuse limit.

**Examples**

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp dampening 20 800 2500 80 25
```

**Related Commands**

N/A

7.6.13 bgp default local-preference

**Command Purpose**

Use this command to change the default local preference value. Use the no parameter with this command to revert to the default setting.

**Command Syntax**

```
bgp default local-preference PREF_VALUE
```
no default local-preference (PREF_VALUE)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PREF_VALUE</td>
<td>Configure default local preference value. The default local preference value is 100.</td>
<td>0-4294967295</td>
</tr>
</tbody>
</table>

**Command Mode**
Router Configuration

**Default**
The default local preference value is 100.

**Usage**
Local preference indicates the preferred path when there are multiple paths to the same destination. The path having a higher preference is preferred. Use bgp default local-preference command to define preference of a particular path. The preference is sent to all routers and access servers in the local autonomous system.

**Examples**
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp default local-preference 234555

**Related Commands**
N/A

**7.6.14 bgp deterministic-med**

**Command Purpose**
Use this command to compare the Multi Exit Discriminator (MED) variable when choosing among routes advertised by different peers in the same autonomous system.
Use the no parameter with this command to disallow this setting.

**Command Syntax**
bgp deterministic-med
no bgp deterministic-med

**Command Mode**
Router Configuration

**Default**
Disabled

**Usage**
"Multi Exit Discriminator (MED) is used in best path selection by BGP. MED is compared after BGP attributes weight, local preference, AS-path and origin have been compared and are equal. Enable bgp deterministic med command on all routers in the local AS, for a correct comparison result. After enabling this command, all paths for the same prefix are grouped together and arranged according to their MED value.
Based on this comparison, the best path is then chosen.
This command compares MED variable when choosing routes advertised by different peers in the same AS, to compare MED, when choosing routes from neighbors in different ASs use the bgp always-compare-med command."

**Examples**
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp deterministic-med
Related Commands

show bgp ipv6, show bgp ipv6 neighbors

7.6.15  bgp enforce-first-as

Command Purpose

Use this command to specifies that any updates received from an external neighbor that do not have the neighbor's configured Autonomous System (AS) at the beginning of the AS_PATH in the received update must be denied. Use the no parameter with this command to disable this feature.

Command Syntax

bgp enforce-first-as
no bgp enforce-first-as

Command Mode

Router Configuration

Default

Disabled

Usage

Enabling this feature adds to the security of the BGP network by not allowing traffic from unauthorized systems.

Examples

Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp enforce-first-as

Related Commands

N/A

7.6.16  bgp fast-external-failover

Command Purpose

Use this command to reset a BGP session immediately, if the interface used for BGP connection goes down. Use the no parameter with this command to disable this feature.

Command Syntax

bgp fast-external-failover
no bgp fast-external-failover

Command Mode

Router Configuration

Default

Enabled

Usage

None

Examples

Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp fast-external-failover
Related Commands

N/A

7.6.17 bgp log-neighbor-changes

Command Purpose

Use this command to enable logging of status change messages without turning on debug bgp commands. Use the no parameter with this command to disable this feature.

Command Syntax

bgp log-neighbor-changes
no bgp log-neighbor-changes

Command Mode

Router Configuration

Default

Disabled

Usage

System implementation provides other kinds of logging services for neighbor status, for example, debug bgp fsm, debug bgp events, etc. However, these commands create a significant hit in the logging performance. The bgp log-neighbor-changes command, logs the following events:

- BGP Notification Received
- Erroneous BGP Update Received
- User reset request
- Peer time-out
- Peer Closing down the session
- Interface flap
- Router ID changed
- Neighbor deleted
- Member added to peer group
- Administrative shutdown
- Remote AS changed
- RR client configuration modification
- Soft reconfiguration modification

Examples

Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp log-neighbor-changes

Related Commands

N/A

7.6.18 bgp router-id

Command Purpose

Use this command to configure the router identifier. Use the no parameter with this command to disable this function.
Command Syntax

bgp router-id ROUTERID
no bgp router-id ( ROUTERID | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROUTERID</td>
<td>A.B.C.D Manually configured router ID.</td>
<td>In IPv4 Address format</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration
Address Family Configuration

Default

In case the loopback interface is configured the router-id is set to the IP address of a loopback interface. If not, the highest IP address is the router-id.

Usage

Use bgp router-id command to manually configure a fixed router ID as a BGP router identifier.

Examples

Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp router-id 1.1.2.3

Related Commands

N/A

7.6.19 bgp scan-time

Command Purpose

Use this command to set the interval for BGP route next-hop scanning. Use the no parameter with this command to disable this function.

Command Syntax

bgp scan-time TIME
no bgp scan-time ( TIME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIME</td>
<td>Scanning interval in seconds. The default scanning interval is 60 seconds.</td>
<td>0-60</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

N/A

Usage

Use this command to configure scanning intervals of BGP routers. This interval is the period after which router checks the validity of the routes in its database. To disable BGP scanning, set the scan time interval to 0 seconds.

Examples

Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp scan-time 10
Related Commands

N/A

7.6.20 clear bgp ipv6 *

Command Purpose

Use this command to reset a BGP connection for all peers.

Command Syntax

clear bgp ipv6 * ( in | out | soft )
clear bgp ipv6 * vrf NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>clears all bgp peers</td>
<td>-</td>
</tr>
<tr>
<td>in</td>
<td>Indicates that incoming advertised routes will be cleared</td>
<td>-</td>
</tr>
<tr>
<td>out</td>
<td>Indicates that outgoing advertised routes will be cleared.</td>
<td>-</td>
</tr>
<tr>
<td>soft</td>
<td>soft (in</td>
<td>out</td>
</tr>
<tr>
<td>vrf</td>
<td>VPN routing/forwarding instance</td>
<td>-</td>
</tr>
<tr>
<td>NAME</td>
<td>VPN Routing/Forwarding instance name</td>
<td>Up to 16 characters</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

N/A

Usage

There are two kinds BGP reset, hard reset will clear BGP peers and establish again. Soft reset only refresh routing table.

Examples

Switch# clear bgp ipv6 *
Switch# clear bgp ipv6 * soft
Switch# clear bgp ipv6 * vrf aa

Related Commands

N/A

7.6.21 clear bgp ipv6 X::X::X

Command Purpose

Use this command to reset a IPv6 BGP connection for a specific IPv6 address.

Command Syntax

clear bgp ipv6 X::X::X ( in | out | soft )
clear ipv6 bgp X::X::X vrf NAME
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>X:X::X:X</td>
<td>Specifies the IPv6 address of the BGP route to be cleared</td>
<td>IPv6 address</td>
</tr>
<tr>
<td>in</td>
<td>Indicates that incoming advertised routes will be cleared</td>
<td>-</td>
</tr>
<tr>
<td>out</td>
<td>Indicates that outgoing advertised routes will be cleared</td>
<td>-</td>
</tr>
<tr>
<td>soft</td>
<td>soft (in</td>
<td>out) Indicates that both incoming and outgoing routes will be cleared</td>
</tr>
<tr>
<td>vrf</td>
<td>VPN routing/forwarding instance</td>
<td>-</td>
</tr>
<tr>
<td>NAME</td>
<td>VPN Routing/Forwarding instance name</td>
<td>Up to 16 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

N/A

**Usage**

N/A

**Examples**

Switch# clear bgp ipv6 2018:1
Switch# clear bgp ipv6 2018:1 soft

**Related Commands**

N/A

7.6.22 clear bgp ipv6 unicast dampening

**Command Purpose**

Use this command to reset all dampened BGP routes under the specified address family.

**Command Syntax**

```
clear bgp ipv6 dampening ( X:X::X | X:X::X/M )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>X:X::X:X</td>
<td>Specifies the IPv6 address for which Bgp dampening is to be cleared.</td>
<td>IPv6 address</td>
</tr>
<tr>
<td>X:X::X::X/M</td>
<td>Specifies the IPv6 address with mask for which Bgp dampening is to be cleared.</td>
<td>IPv6 address with mask length</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

N/A

**Usage**

N/A
Examples

Switch# clear bgp ipv6 unicast dampening
Switch# clear bgp ipv6 unicast dampening 2018::1

Related Commands

N/A

7.6.23 clear bgp ipv6 unicast flap-statistics

Command Purpose

Use this command to clear the flap count and history duration for all the prefixes under the specified address family.

Command Syntax

clear bgp ipv6 unicast flap-statistics (X:X::X | X:X::X/M )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>X:X::X</td>
<td>Specifies the IPv6 address for which Bgp dampening is to be cleared.</td>
<td>IPv6 address</td>
</tr>
<tr>
<td>X:X::X/X/M</td>
<td>Specifies the IPv6 address with mask for which Bgp dampening is to be cleared.</td>
<td>IPv6 address with mask length</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

Switch# clear bgp ipv6 unicast flap-statistics 10.10.0.121

Related Commands

N/A

7.6.24 clear bgp ipv6 ASN

Command Purpose

Use this command to reset a BGP connection for all peers in a specified Autonomous System.

Command Syntax

clear bgp ipv6 ASN (in | out | soft )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASN</td>
<td>Specifies the AS Number for which all routes will be cleared</td>
<td>1-4294967295</td>
</tr>
<tr>
<td>in</td>
<td>Indicates that incoming advertised routes will be cleared</td>
<td>-</td>
</tr>
<tr>
<td>out</td>
<td>Indicates that outgoing advertised routes will be cleared.</td>
<td>-</td>
</tr>
<tr>
<td>soft</td>
<td>soft (in</td>
<td>out) Indicates that both incoming and outgoing routes will be cleared</td>
</tr>
</tbody>
</table>
### Command Mode
Privileged EXEC

### Default
N/A

### Usage
N/A

### Examples
Switch# clear bgp ipv6 100

### Related Commands
N/A

#### 7.6.25 clear bgp ipv6 external

**Command Purpose**
Use this command to reset a BGP connection for all external peers.

**Command Syntax**
clear bgp ipv6 external (in | soft |)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>external</td>
<td>Clears all external peers</td>
<td>-</td>
</tr>
<tr>
<td>in</td>
<td>Indicates that incoming advertised routes will be cleared</td>
<td>-</td>
</tr>
<tr>
<td>soft</td>
<td>soft (in</td>
<td>out) Indicates that both incoming and outgoing routes will be cleared</td>
</tr>
</tbody>
</table>

### Command Mode
Privileged EXEC

### Default
N/A

### Usage
N/A

### Examples
Switch# clear bgp ipv6 external in

### Related Commands
N/A

#### 7.6.26 clear bgp ipv6 peer-group

**Command Purpose**
Use this command to reset a BGP connection for all members of a peer group.

**Command Syntax**
clear bgp ipv6 peer-group WORD (in | out | soft |)

---
### clear bgp ipv6 peer-group

**Parameter** | **Parameter Description** | **Parameter Value**  
--- | --- | ---  
peer-group | Clears all members of a peer group |  
WORD | Specifies the name of the peer group for which all members will be cleared. | Up to 20 characters  
in | Indicates that incoming advertised routes will be cleared |  
out | Indicates that outgoing advertised routes will be cleared. |  
soft | soft (in|out) Indicates that both incoming and outgoing routes will be cleared |  

**Command Mode**
Privileged EXEC

**Default**
N/A

**Usage**
None

**Examples**
Switch# clear bgp ipv6 peer-group Peer1 out

### debug bgp

**Command Purpose**
Use this command to specify all debugging options for BGP. Use the no parameter with this command to disable this function.

**Command Syntax**
d debug bgp (all | dampening | events | filters | fsm | keepalives | mpls | updates)  
no debug bgp (all | dampening | events | filters | fsm | keepalives | mpls | nsm | updates)

| Parameter | Parameter Description | Parameter Value  
--- | --- | ---  
all | Used with the no form exclusively; turns off all debugging for BGP |  
dampening | Specifies debugging for BGP dampening. |  
events | Specifies debugging for BGP events. |  
filters | Specifies debugging for BGP filters. |  
fsm | Specifies debugging for BGP Finite State Machine (FSM). |  
mpls | Specifies debugging for BGP Multiprotocol Label Switching. |  
keepalives | Specifies debugging for BGP keepalives. |  
updates | Specifies debugging for BGP updates. |  

**Command Mode**
Privileged EXEC
**Default**

N/A

**Usage**

This command without any parameters turns on normal bgp debug information.

**Examples**

```
Switch# debug bgp
Switch# debug bgp events
```

**Related Commands**

N/A

---

**7.6.28 exit-address-family**

**Command Purpose**

Use this command to exit the address family mode.

**Command Syntax**

```
exit-address-family
```

**Command Mode**

Address Family Configuration

**Default**

N/A

**Usage**

N/A

**Examples**

The following example shows the use of exit-address-family command and the change in the prompt after using this command:

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# address-family ipv6
Switch(config-router-af)# exit-address-family
Switch(config-router-af)#ab
```

**Related Commands**

address-family

---

**7.6.29 neighbor activate**

**Command Purpose**

Use this command to enable the exchange of the specified AF routes with a neighboring router. Use the no parameter with this command to disable exchange of information with a neighbor.

**Command Syntax**

```
neighbor NEIGHBORID activate
no neighbor NEIGHBORID activate
```
### Command Mode

**Router Configuration**

**Address Family Configuration**

**Default**

N/A

**Usage**

After the TCP connection is opened with the neighbor, this command is used to enable or disable the exchange of the specified AF information with a neighboring router. To enable the exchange of multicast and VPNv4 address prefix types, neighbors are activated using the neighbor activate command in address family mode.

**Examples**

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 active
```

**Related Commands**

neighbor remote-as

7.6.30 neighbor advertisement-interval

**Command Purpose**

Use this command to set the minimum interval between sending the BGP routing updates. Use the no parameter with this command to set the interval time to default.

**Command Syntax**

```
neighbor NEIGHBORID advertise-interval TIME
no neighbor NEIGHBORID advertise-interval TIME
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(X:X::X</td>
<td>TAG)</td>
</tr>
<tr>
<td>X::X::X::X</td>
<td>Specifies the address of the BGP neighbor in IPv6 format.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>-</td>
</tr>
<tr>
<td>TIME</td>
<td>Advertise-interval value in seconds</td>
<td>0-600</td>
</tr>
</tbody>
</table>
Command Mode
Router Configuration

Default
N/A

Usage
Use this command to set the minimum interval between the sending of BGP routing updates. To reduce the flapping of routes to internet, a minimum advertisement interval is set, so that the BGP routing updates are sent only per interval seconds. bgp dampening can also be used to control the effects of flapping routes.

Examples
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 2018::1 advertisement-interval 45

Related Commands
N/A

7.6.31 neighbor allowas-in

Command Purpose
Use this command to configure PE routers to allow re-advertisement of all prefixes containing duplicate Autonomous System Numbers (ASNs). Use the no parameter with this command to disable the readvertisement of a PE router’s ASN.

Command Syntax
neighbor NEIGHBOR allowas-in [NUMBER ]
no neighbor NEIGHBOR allowas-in

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(X:X::X)(TAG)</td>
<td>-</td>
</tr>
<tr>
<td>X:X::X:X</td>
<td>Specifies the address of the BGP neighbor in IPv6 format.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>NUMBER</td>
<td>Number of occurrences of AS number. Default value is 1</td>
<td>1-10</td>
</tr>
</tbody>
</table>

Command Mode
Address Family Configuration

Default
Disabled

Usage
In a hub and spoke configuration, a PE router re-advertises all prefixes containing duplicate ASNs. Use the neighbor allowas-in command to configure two VRFs on each PE router to receive and re-advertise prefixes. One of the VRFs receives prefixes with ASNs from all PE routers and then advertises them to neighboring PE routers. The other VRF receives prefixes with ASNs from the CE router and re-advertises them to all PE routers in the hub and spoke configuration. Control the number of times an ASN is advertised, by specifying a number from 1 to 10.
Examples

Switch# configure terminal
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 allowas-in 3

Related Commands

N/A

7.6.32 neighbor attribute-unchanged

Command Purpose

Use this command to advertise unchanged BGP attributes to the specified neighbor. Use the no parameter with this command to disable this function.

Command Syntax

neighbor NEIGHBORID attribute-unchanged { as-path | next-hop | med }
no neighbor NEIGHBORID attribute-unchanged { as-path | next-hop | med }

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(X:X::X)(TAG)</td>
<td>-</td>
</tr>
<tr>
<td>X:X::X:X</td>
<td>Specifies the address of the BGP neighbor in IPv6 format.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>as-path</td>
<td>AS path attribute</td>
<td>-</td>
</tr>
<tr>
<td>next-hop</td>
<td>Next hop attribute</td>
<td>-</td>
</tr>
<tr>
<td>med</td>
<td>Multi Exit Discriminator</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Address Family Configuration

Default

N/A

Usage

N/A

Examples

Switch# configure terminal
Switch(config-router)# router bgp 10
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 23018::1 attribute-unchanged as-path med

Related Commands

N/A

7.6.33 neighbor capability orf prefix-list

Command Purpose

Use this command to advertise ORF capability to neighbors. Use the no parameter with this command to disable this function.
Command Syntax

neighbor NEIGHBORID capability orf prefix-list (both | receive | send)
no neighbor NEIGHBORID capability orf prefix-list (both | receive | send)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(X:X::X:TAG)</td>
<td>-</td>
</tr>
<tr>
<td>X:X::X</td>
<td>Specifies the address of the BGP neighbor in IPv6 format.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>orf</td>
<td>Advertises ORF capability to its neighbors</td>
<td>-</td>
</tr>
<tr>
<td>both</td>
<td>Indicates that the local router can send ORF entries to its peer as well as receive ORF entries from its peer.</td>
<td>-</td>
</tr>
<tr>
<td>receive</td>
<td>Indicates that the local router is willing to receive ORF entries from its peer</td>
<td>-</td>
</tr>
<tr>
<td>send</td>
<td>Indicates that the local router is willing to send ORF entries to its peer</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Address Family Configuration

Default
N/A

Usage
Outbound Route Filters (ORFs) send and receive capabilities to lessen the number of updates exchanged between neighbors. By filtering updates, this option minimizes generating and processing of updates. The local router advertises the ORF capability in send mode and the remote router receives the ORF capability in receive mode applying the filter as outbound policy. The two routers exchange updates to maintain the ORF for each

Examples

<table>
<thead>
<tr>
<th>Switch# configure terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# router bgp 10</td>
</tr>
<tr>
<td>Switch(config-router)# address-family ipv6</td>
</tr>
<tr>
<td>Switch(config-router-af)# neighbor 1.1.1.1 capability orf prefix-list both</td>
</tr>
</tbody>
</table>

Related Commands
N/A

7.6.34 neighbor default-originate

Command Purpose
Use this command to allow a BGP local router to send the default route 0:0:0:0 to a neighbor for use as a default route. Use the no parameter with this command to send no route as a default.

Command Syntax

neighbor NEIGHBORID default-originate (ROUTemap | )
nno neighbor NEIGHBORID default-originate (ROUTemap | )
### NEIGHBORID

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>(X:X::X)</td>
<td>Specifies the address of the BGP neighbor in IPv6 format.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>ROUTEMAP</td>
<td>route-map WORD</td>
<td>-</td>
</tr>
<tr>
<td>route-map</td>
<td>The route-map to specify criteria to originate default routes</td>
<td>-</td>
</tr>
<tr>
<td>WORD</td>
<td>Route-map name</td>
<td>-</td>
</tr>
</tbody>
</table>

### Command Mode

Address Family Configuration

### Default

N/A

### Usage

Every router should have a default route, it is used to send datas to the network which is not existent in local RIB. To set a default route on each router can make every router have a default route, or to create a default route and broadcast it to BGP peer by this command.

### Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 default-originate route-map myroute
```

### Related Commands

N/A

#### 7.6.35 neighbor description

### Command Purpose

Use this command to associate a description with a neighbor.
Use the no parameter with this command to remove the description.

### Command Syntax

```
neighbor NEIGHBORID description LINE
no neighbor NEIGHBORID description
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>(X:X::X)</td>
<td>Specifies the address of the BGP neighbor in IPv6 format.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>LINE</td>
<td>Text to describing the neighbor.</td>
<td>Up to 80 characters</td>
</tr>
</tbody>
</table>
**Command Mode**

Router Configuration

**Default**

N/A

**Usage**

None

**Examples**

Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 2018::1 description Backup router for sales.

**Related Commands**

N/A

7.6.36 **neighbor distribute-list**

**Command Purpose**

Use this command to filter route update from a particular BGP neighbor. Use the no parameter with this command to remove an entry.

**Command Syntax**

neighbor NEIGHBORID distribute-list WORD (in | out)
no neighbor NEIGHBORID distribute-list WORD (in | out)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(XX::X:X</td>
<td>TAG)</td>
</tr>
<tr>
<td>X::X::X</td>
<td>Specifies the address of the BGP neighbor in IPv6 format.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
<td></td>
</tr>
<tr>
<td>TAG</td>
<td>WORD</td>
<td>The name of IP access-list Up to 20 characters</td>
</tr>
<tr>
<td>in</td>
<td>Indicates that incoming advertised routes will be filtered.</td>
<td>-</td>
</tr>
<tr>
<td>out</td>
<td>Indicates that outgoing advertised routes will be filtered.</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Address Family Configuration

**Default**

N/A

**Usage**

Use only one distribute-list per BGP neighbor.

**Examples**

Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 distribute-list mylist out
Related Commands

N/A

7.6.37 neighbor ebgp-multihop

Command Purpose

Use this command to accept and attempt BGP connections to external peers on indirectly connected networks.
Use the no parameter with this command to return to the default.

Command Syntax

neighbor NEIGHBORID ebgp-multihop (COUNT)
no neighbor NEIGHBORID ebgp-multihop

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(X:X::X:TAG)</td>
<td>-</td>
</tr>
<tr>
<td>X:X::X:X</td>
<td>Specifies the address of the BGP neighbor in IPv6 format.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td></td>
<td>the neighbor peer-group and neighbor remote-as commands. When this parameter is used</td>
<td></td>
</tr>
<tr>
<td></td>
<td>with a command, the command applies on all peers in the specified group.</td>
<td></td>
</tr>
<tr>
<td>COUNT</td>
<td>Maximum hop count. If the maximum hop count is not set the hop count is 255.</td>
<td>1-255</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

N/A

Usage

Multihop is not established if the only route to the multihop peer is a default route. This avoids loop formation.

Examples

Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 2018::1 remote-as 20
Switch(config-router)# neighbor 2018::1 ebgp-multihop 5

Related Commands

N/A

7.6.38 neighbor filter-list

Command Purpose

Use this command to set up a BGP filter.
Use the no parameter with this command to disable this function.

Command Syntax

neighbor NEIGHBORID filter-list LISTNAME (in | out)
no neighbor NEIGHBORID filter-list LISTNAME (in | out)
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(X:X::X:X</td>
<td>TAG)</td>
</tr>
<tr>
<td>X:X::X:X</td>
<td>Specifies the address of the BGP neighbor in IPv6 format.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>in</td>
<td>Indicates that incoming advertised routes will be filtered.</td>
<td>-</td>
</tr>
<tr>
<td>out</td>
<td>Indicates that outgoing advertised routes will be filtered.</td>
<td>-</td>
</tr>
<tr>
<td>LISTNAME</td>
<td>The name of an autonomous system path access list.</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Address Family Configuration

**Default**

N/A

**Usage**

This command specifies an access list filter on updates based on the BGP autonomous system paths. Each filter is an access list based on regular expressions.

**Examples**

Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 filter-list listname out

**Related Commands**

N/A

**7.6.39 neighbor maximum-prefix**

**Command Purpose**

Use this command to control the number of prefixes that can be received from a neighbor. Use the no parameter with this command to disable this function.

**Command Syntax**

neighbor NEIGHBORID maximum-prefix MAXIMUM
no neighbor NEIGHBORID maximum-prefix

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(X:X::X:X</td>
<td>TAG)</td>
</tr>
<tr>
<td>X:X::X:X</td>
<td>Specifies the address of the BGP neighbor in IPv6 format.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>MAXIMUM</td>
<td>MAXPREFIX (THRESHOLD) (warning-only)</td>
<td>-</td>
</tr>
<tr>
<td>MAXPREFIX</td>
<td>Specifies the maximum number of prefixes permitted.</td>
<td>1-4294967295</td>
</tr>
<tr>
<td>THRESHOLD</td>
<td>&lt;1-100&gt; Specifies the threshold value, 1 to 100 percent.</td>
<td>1-100</td>
</tr>
<tr>
<td>warning-only</td>
<td>Only gives a warning message when the limit is exceeded.</td>
<td>-</td>
</tr>
</tbody>
</table>
Command Mode
Address Family Configuration

Default
N/A

Usage
The neighbor maximum-prefix command allows the configuration of a specified number of prefixes that a BGP router is allowed to receive from a neighbor. When the warning-only option is not used, if any extra prefixes are received, the router ends the peering. A terminated peer, stays down until the clear ip bgp command is used.

Examples

Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 maximum-prefix 1244 warning-only

Related Commands
N/A

7.6.40 neighbor next-hop-self

Command Purpose
Use this command to configure the router as the next hop for a BGP-speaking neighbor or peer group. Use the no parameter with this command to disable this feature.

Command Syntax

neighbor NEIGHBORID next-hop-self
no neighbor NEIGHBORID next-hop-self

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(X:X::X:X</td>
<td>TAG)</td>
</tr>
<tr>
<td>X::X::X</td>
<td>Specifies the address of the BGP neighbor in IPv6 format.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td></td>
<td>create peer groups, refer to the neighbor peer-group and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>neighbor remote-as commands. When this parameter is used</td>
<td></td>
</tr>
<tr>
<td></td>
<td>with a command, the command applies on all peers in the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>specified group.</td>
<td></td>
</tr>
</tbody>
</table>

Command Mode
Address Family Configuration

Default
N/A

Usage
This command allows a BGP router to change the nexthop information that is sent to the iBGP peer. The nexthop information is set to the IP address of the interface used to communicate with the neighbor.

Examples

Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 10.10.0.72 next-hop-self
Related Commands

N/A

7.6.41 neighbor override-capability

Command Purpose

Use this command to override a capability negotiation result.
Use the no parameter with this command to disable this function

Command Syntax

neighbor NEIGHBORID override-capability
no neighbor NEIGHBORID override-capability

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(X:X::X:TAG)</td>
<td>-</td>
</tr>
<tr>
<td>X:X::X:</td>
<td>Specifies the address of the BGP neighbor in IPv6 format.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

N/A

Usage

None

Examples

Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# neighbor 2018::1 override-capability

Related Commands

N/A

7.6.42 neighbor passive

Command Purpose

Use this command to set a BGP neighbor as passive.
Use the no parameter with this command to disable this function

Command Syntax

( no ) neighbor NEIGHBORID passive
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(X:X::X:TAG) Specifies the address of the BGP neighbor in IPv6 format.</td>
<td></td>
</tr>
<tr>
<td>X:X::X:X</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>IPv6 Address</td>
</tr>
</tbody>
</table>

### Command Mode

**Router Configuration**

**Default**

N/A

**Usage**

N/A

**Examples**

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# neighbor 2018::1 passive
```

**Related Commands**

N/A

7.6.43 `neighbor peer-group (adding a neighbor)`

**Command Purpose**

Use this command to add a neighbor to an existing peer-group. Use the no parameter with this command to disable this function.

**Command Syntax**

```
neighbor IPADDRESS peer-group TAG
no neighbor IPADDRESS peer-group
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPV6_ADDR</td>
<td>X:XX::X:X Specifies the address of the BGP neighbor in IPv6 format.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td></td>
<td>XX::X:X Specifies the address of the BGP neighbor in IPv6 format.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TAG Name of the peer-group</td>
<td></td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

**Router Configuration**

**Default**

N/A
Usage

Use this command to Neighbors with the same update policies are grouped into peer groups. This facilitates the updates of various policies, such as, distribute and filter lists. The peer-group is then configured easily with any of the neighbor commands. Any changes made to the peer group affect all members.

To create a peer-group use the neighbor peer-group create command and then use this command to add neighbors to the group.

Examples

This example shows a new peer-group group1 and the adding of a neighbor 2018::1 to the group:

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor group1 peer-group
Switch(config-router)# neighbor 2018::1 peer-group group1
```

Related Commands

N/A

7.6.44 neighbor peer-group (creating a peer-group)

Command Purpose

Use this command to create a peer-group.
Use the no parameter with this command to disable this function

Command Syntax

```
neighbor TAG peer-group
no neighbor TAG peer-group
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TAG</td>
<td>Name of the peer-group</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

N/A

Usage

Neighbors with the same update policies are grouped into peer groups. This facilitates the updates of various policies, such as, distribute and filter lists. The peer-group is then configured easily with any of the neighbor commands. Any changes made to the peer group affect all members. Use this command to create a peer-group.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor group1 peer-group
```

Related Commands

N/A

7.6.45 neighbor prefix-list

Command Purpose

Use this command to distribute BGP neighbor information as specified in a prefix list.
Use the no parameter with this command to remove an entry.

Command Syntax

```
neighbor NEIGHBORID prefix-list LISTNAME ( in | out )
no neighbor NEIGHBORID prefix-list LISTNAME ( in | out )
```
### Command Mode

Address Family Configuration

### Default

N/A

### Usage

Use this command to specify a prefix list for filtering BGP advertisements. Filtering by prefix list matches the prefixes of routes with those listed in the prefix list. If there is a match, the route is used. An empty prefix list permits all prefixes. If a given prefix does not match any entries of a prefix list, the route is denied access. When multiple entries of a prefix list match a prefix, the entry with the smallest sequence number is considered to be a real match.

The router begins the search at the top of the prefix list, with the sequence number 1. Once a match or deny occurs, the router does not need to go through the rest of the prefix list. For efficiency the most common matches or denies are listed at the top. The neighbor distribute-list command is an alternative to the neighbor prefix-list command and only one of them can be used for filtering to the same neighbor in any direction.

### Examples

Switch# configure terminal
Switch(config)# ip prefix-list list1 deny 30.0.0.0/24
Switch(config)# router bgp 12
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 10.10.10.10 prefix-list list1 in

### Related Commands

ip prefix-list

### 7.6.46 neighbor remote-as

#### Command Purpose

Use this command to configure an internal or external BGP (iBGP or eBGP) TCP session with another router.

#### Command Syntax

neighbor NEIGHBORID remote-as ASNUM
no neighbor NEIGHBORID remote-as ASNUM

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(X::X::X</td>
<td>TAG)</td>
</tr>
<tr>
<td>X::X::X</td>
<td>Specifies the address of the BGP neighbor in IPv6 format.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>LISTNAME</td>
<td>The number of an AS-path access list.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>in</td>
<td>Specifies that the access list applies to incoming advertisements.</td>
<td>-</td>
</tr>
<tr>
<td>out</td>
<td>Specifies that the access list applies to outgoing advertisements.</td>
<td>-</td>
</tr>
</tbody>
</table>
### Command Mode

**Router Configuration**

**Default**

N/A

**Usage**

This command is used to configure iBGP and eBGP sessions with other neighbors. A peer-group support of this command is configured only after creating a specific peer-group.

**Examples**

Switch# configure terminal
Switch(config)# router bgp 11
Switch(config-router)# neighbor 2018::1 remote-as 345

**Related Commands**

N/A

7.6.47 `neighbor remove-private-AS`

**Command Purpose**

Use this command to remove the private Autonomous System (AS) number from outbound updates. Use the no parameter with this command too revert to default.

**Command Syntax**

```
neighbor NEIGHBORID remove-private-AS
no neighbor NEIGHBORID remove-private-AS
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASNUM</td>
<td>Neighbor’s autonomous system number</td>
<td>1-4294967295</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(X:X::X)[TAG]</td>
<td>-</td>
</tr>
<tr>
<td>X:X::X</td>
<td>Specifies the address of the BGP neighbor in IPv6 format.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Address Family Configuration
Default
 Disabled

Usage
The private AS numbers range from <64512-65535>. Private AS numbers are not advertised to the Internet. This command is used with external BGP peers only. The router removes the AS numbers only if the update includes private AS numbers. If the update includes both private and public AS numbers, the system treats it as an error.

Examples

Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 remove-private-AS

Related Commands
N/A

7.6.48 neighbor route-reflector-client

Command Purpose
Use this command to configure the router as a BGP route reflector and configure the specified neighbor as its client. Use the no parameter with this command to indicate that the neighbor is not a client.

Command Syntax
neighbor NEIGHBORID route-reflector-client
no neighbor NEIGHBORID route-reflector-client

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(X:X::X:TAG)</td>
<td>-</td>
</tr>
<tr>
<td>X::X::X</td>
<td>Specifies the address of the BGP neighbor in IPv6 format.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode
Address Family Configuration

Default
N/A

Usage
Route reflectors are a solution for the explosion of iBGP peering within an autonomous system. By route reflection the number of iBGP peers within an AS is reduced. Use the neighbor route-reflector-client command to configure the local router as the route reflector and specify neighbors as its client. An AS can have more than one route reflector. One route reflector treats the other route reflector as another iBGP speaker.

Examples

Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 route-reflector-client

Related Commands
N/A
7.6.49  neighbor send-community

Command Purpose
Use this command to specify that a community attribute should be sent to a BGP neighbor. Use the no parameter with this command to remove the entry. Use the extended and no parameters to remove extended communities. Specifying no other parameter means standard communities only.

Command Syntax
neighbor NEIGHBORID send-community ( both | extended | standard )
no neighbor NEIGHBORID send-community ( both | extended | standard )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(X:X::X:TAG)</td>
<td>-</td>
</tr>
<tr>
<td>X:X::X:</td>
<td>Specifies the address of the BGP neighbor in IPv6 format.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td></td>
<td>create peer groups, refer to the neighbor peer-group and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>neighbor remote-as commands. When this parameter is used</td>
<td></td>
</tr>
<tr>
<td></td>
<td>with a command, the command applies on all peers in the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>specified group.</td>
<td></td>
</tr>
<tr>
<td>both</td>
<td>Sends Standard and Extended Community attributes</td>
<td>-</td>
</tr>
<tr>
<td>extended</td>
<td>Sends Extended Community attributes</td>
<td>-</td>
</tr>
<tr>
<td>standard</td>
<td>Sends Standard Community attributes</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Address Family Configuration

Default
None

Usage
By default, community attributes are not sent to a neighbor. To use this command to enable this command. Route-map can be based on neighbor address, peer group name or AS path information.

Examples
Switch# configure terminal
Switch(config)# bgp config-type standard
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 send-community extended

Related Commands
N/A

7.6.50  neighbor shutdown

Command Purpose
Use this command to disable a neighbor. Use the no parameter with this command to re-enable the neighbor.

Command Syntax
neighbor NEIGHBORID shutdown
no neighbor NEIGHBORID shutdown
Parameter | Parameter Description | Parameter Value
--- | --- | ---
NEIGHBORID | (X:X::X:X|TAG) | -
A.B.C.D | Specifies the address of the BGP neighbor in IPv6 format. | IPv6 Address
TAG | Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group. | Up to 20 characters

Command Mode
Router Configuration

Default
N/A

Usage
This command shuts down any active session for the specified neighbor and clears all related routing data.

Examples
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 2018::1 shutdown

Related Commands
N/A

7.6.51 neighbor soft-reconfiguration inbound

Command Purpose
Use this command to configure to start storing updates. Use the no parameter with this command to disable this function.

Command Syntax
neighbor NEIGHBORID soft-reconfiguration inbound
bo neighbor NEIGHBORID soft-reconfiguration inbound

Parameter | Parameter Description | Parameter Value
--- | --- | ---
NEIGHBORID | (X:X::X:X|TAG) | -
X:X::X | Specifies the address of the BGP neighbor in IPv4 format. | IPv6 Address
TAG | Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group. | Up to 20 characters

Command Mode
Router Configuration
Address Family Configuration

Default
N/A
Usage

Use this command to store updates for inbound soft reconfiguration. Soft-reconfiguration may be used in lieu of BGP route refresh capability. Using this command enables local storage of all the received routes and their attributes. This requires additional memory. When a soft reset (inbound) is done on this neighbor, the locally stored routes are reprocessed according to the inbound policy. The BGP neighbor connection is not affected.

Examples

Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 soft-reconfiguration inbound

Related Commands

N/A

7.6.52 neighbor strict-capability-match

Command Purpose

Use this command to close the BGP connection if capability value does not completely match to remote peer. Use the no parameter with this command to disable this function.

Command Syntax

neighbor NEIGHBORID strict-capability-match
no neighbor NEIGHBORID strict-capability-match

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(X:X::X:TAG)</td>
<td>-</td>
</tr>
<tr>
<td>X:X::X:X</td>
<td>Specifies the address of the BGP neighbor in IPv6 format.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer-groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode

Router Configuration

Default

N/A

Usage

N/A

Examples

Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 strict-capability-match

Related Commands

N/A
### 7.6.53 neighbor timers

#### Command Purpose
Use this command to set the timers for a specific BGP neighbor.
Use the no parameter with this command to clear the timers for a specific BGP neighbor.

#### Command Syntax
```
neighbor NEIGHBORID timers KEEPALIVE HOLDTIME
no neighbor NEIGHBORID timers
```

#### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>Specifies the address of the BGP neighbor in IPv6 format.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>X:X::X:X</td>
<td>Specifies the address of the BGP neighbor in IPv6 format.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer</td>
<td>Up to 20</td>
</tr>
<tr>
<td></td>
<td>groups, refer to the neighbor peer-group and neighbor remote-as</td>
<td>characters</td>
</tr>
<tr>
<td></td>
<td>commands. When this parameter is used with a command, the command</td>
<td></td>
</tr>
<tr>
<td></td>
<td>applies on all peers in the specified group.</td>
<td></td>
</tr>
<tr>
<td>KEEPALIVE</td>
<td>Frequency (in seconds) at which a router sends keepalive messages to its</td>
<td>1-65535</td>
</tr>
<tr>
<td></td>
<td>neighbor. The default is 60 seconds.</td>
<td></td>
</tr>
<tr>
<td>HOLDTIME</td>
<td>Interval (in seconds) after which, on not receiving a keepalive message,</td>
<td>3-65535</td>
</tr>
<tr>
<td></td>
<td>the router declares a neighbor dead. The default is 180 seconds.</td>
<td></td>
</tr>
</tbody>
</table>

#### Command Mode
Router Configuration

#### Default
N/A

#### Usage
Keepalive messages are sent by a router to inform another router that the BGP connection between the two is still active. The keepalive interval is the period of time between each keepalive message sent by the router. The holdtime interval is the time the router waits to receive a keepalive message and if it does not receive a message for this period it declares the neighbor dead.

#### Examples
```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 timers 60 120
```

#### Related Commands
N/A

### 7.6.54 neighbor unsuppress-map

#### Command Purpose
Use this command to selectively leak more-specific routes to a particular neighbor.

#### Command Syntax
```
neighbor NEIGHBORID unsuppress-map WORD
no neighbor NEIGHBORID unsuppress-map WORD
```
### Parameter | Parameter Description | Parameter Value
---|---|---
**NEIGHBORID** (X:X::X:X|TAG) | - |
**X::X::X** | Specifies the address of the BGP neighbor in IPv6 format. | IPv6 Address |
**TAG** | Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group. | Up to 20 characters |
**WORD** | Name of route map | - |

**Command Mode**
Address Family Configuration

**Default**
N/A

**Usage**
When the aggregate-address command is used with the summary-only option, the more-specific routes of the aggregate are suppressed to all neighbors. Use the unsuppress-map command to selectively leak more-specific routes to a particular neighbor.

**Examples**
```
Switch# configure terminal
Switch(config)#router bgp 10
Switch(config-router)#address-family ipv6
Switch(config-router-af)#neighbor 2018::1 unsuppress-map mymap
```

**Related Commands**
N/A

7.6.55 neighbor update-source

**Command Purpose**
Use this command to allow internal BGP sessions to use any operational interface for TCP connections. Use the no parameter with this command to restore the interface assignment to the closest interface.

**Command Syntax**
```
neighbor NEIGHBORID update-source IFNAME
no neighbor NEIGHBORID update-source
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NEIGHBORID</strong> (X:X::X:X</td>
<td>TAG)</td>
<td>-</td>
</tr>
<tr>
<td><strong>X::X::X</strong></td>
<td>Specifies the address of the BGP neighbor in IPv6 format.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td><strong>TAG</strong></td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td><strong>IFNAME</strong></td>
<td>Specifies the loopback interface.</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>
Command Mode

Router Configuration

Default
N/A

Usage

Use this command in conjunction with any specified interface on the router. The loopback interface is the interface that is most commonly used with this command. The use of loopback interface eliminates a dependency and BGP does not have to rely on the availability of a particular interface for making TCP connections.

Examples

Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 2018::1 update-source eth-0-1

Related Commands
N/A

7.6.56  neighbor weight

Command Purpose

Use this command to set default weights for routes from this neighbor. Use the no parameter with this command to remove a weight assignment.

Command Syntax

neighbor NEIGHBORID weight WEIGHT
no neighbor NEIGHBORID weight

Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(X:X::X)[TAG]</td>
<td>-</td>
</tr>
<tr>
<td>X:X::X</td>
<td>Specifies the address of the BGP neighbor in IPv6 format.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>WEIGHT</td>
<td>Specifies the weight this command assigns to the route.</td>
<td>0-65535</td>
</tr>
</tbody>
</table>

Command Mode

Address Family Configuration

Default
N/A

Usage

Use this command to specify a weight value to all routes learned from a neighbor. The route with the highest weight gets preference when there are other routes on the network. Unlike the local-preference attribute, the weight attribute is relevant only to the local router. The weights assigned using the set weight command overrides the weights assigned using this command.

Examples

Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)address-family ipv6
Switch(config-router-af)# neighbor 2018::1 weight 60

Related Commands

N/A

7.6.57  network

Command Purpose

Use this command to specify the networks to be advertised by the BGP routing process. A unicast network address without a mask is accepted if it falls into the natural boundary of its class. A class-boundary mask is derived if the address matches its natural class-boundary.

Use the no form of this command to remove a network route entry.

Command Syntax

network X:X::X:X/M
network X:X::X:X/M route-map WORD
no network X:X::X:X/M
no network X:X::X:X/M route-map WORD

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>X:X::X:X/M</td>
<td>IPv6 prefix &lt;network&gt;, e.g., 2018::/64</td>
<td>IPv6 address with mask length</td>
</tr>
<tr>
<td>WORD</td>
<td>Name of the route map</td>
<td>The length of route-map name should not greater than 20 and the first character should be 'a'-'z', 'A'-'Z' or '0'-'9'.</td>
</tr>
</tbody>
</table>

Command Mode

Address Family Configuration

Default

N/A

Usage

N/A

Examples

The following example illustrates a address configured as a network route. The network prefix mask length of 64 will be internally derived, that is, 2018::/64:

```
Switch# configure terminal
Switch(config)#router bgp 1
Switch(config-router)address-family ipv6
Switch(config-router-af)#network 2018::/64
```

! router bgp 1
! no synchronization
! network 2018::/64
!

Related Commands

N/A
7.6.58  network synchronization

**Command Purpose**

Use this command to ensure the exact same static network prefix, specified through any of the network commands, is local or has IGP reachability (in the NSM RIB) before being introduced into the BGP RIB. Use the no parameter with this command to disable this function.

**Command Syntax**

network synchronization
no network synchronization

**Command Mode**

Router Configuration
Address Family Configuration

**Default**

Network synchronization is disabled by default.

**Usage**

N/A

**Examples**

The following example enables IGP synchronization of BGP static network routes in the router configuration mode:

Switch# configure terminal
Switch(config)# router bgp 11
Switch(config-router)# network synchronization

**Related Commands**

N/A

7.6.59  synchronization

**Command Purpose**

Use this command to enable IGP synchronization of Internal BGP (iBGP) learned routes with the Internal Gateway Protocol (IGP) system in the router configuration mode or in the address-family configuration mode. Use the no parameter with this command to disable this function.

**Command Syntax**

synchronization
no synchronization

**Command Mode**

Router Configuration
Address Family Configuration

**Default**

IGP synchronization is disabled.

**Usage**

Synchronization is used when a BGP router should not advertise routes learned from iBGP neighbors, unless those routes are also present in an IGP (for example, OSPF). Synchronization may be enabled when all the routers in an autonomous system do not speak BGP, and the autonomous system is a transit for other autonomous systems. The no synchronization command is used when BGP router can advertise routes learned from its iBGP neighbors without waiting for the IGP reachability to be present.
Examples

The following example enables IGP synchronization of BGP static network routes in the IPv6-Unicast address family:

```
Switch# configure terminal
Switch(config)# router bgp 11
Switch(config)# address-family ipv6
Switch(config-af)# network synchronization
```

Related Commands

N/A

7.6.60  router bgp

Command Purpose

Use this command to configure a BGP routing process. Use the no parameter with this command to disable a routing process.

Command Syntax

```
router bgp ASN  
no router bgp ASN
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASN</td>
<td>Specifies the Autonomous System (AS) number</td>
<td>1-4294967295</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

N/A

Usage

The router bgp command enables a BGP routing process.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)#
```

Related Commands

N/A

7.6.61  show debugging bgp

Command Purpose

Use this command to display the BGP debugging option set.

Command Syntax

```
show debugging bgp
```

Command Mode

Privileged EXEC

Default

N/A
Usage
None

Examples
Switch# show debugging bgp

Related Commands
N/A

7.6.62 show bgp ipv6

Command Purpose
Use this command to display BGP network information.

Command Syntax
show bgp ipv6 (ipaddress |)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>X::X::X::X/X specifies</td>
<td>IPv6 address with mask length</td>
</tr>
<tr>
<td>the address and length.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>unicast</td>
<td>Specifies a IPv4 unicast address family. This is the default option.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
N/A

Usage
N/A

Examples
Switch# show bgp ipv6

Related Commands
N/A

7.6.63 show bgp ipv6 community

Command Purpose
Use this command to display routes matching the communities.

Command Syntax
show bgp (ipv6 | community | AA:NN | local-AS | no-advertise | no-export |) | (exact-match |) |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>local-AS</td>
<td>Do not send outside local AS (well-known community).</td>
<td>-</td>
</tr>
<tr>
<td>AA:NN</td>
<td>Specifies the valid value for the community number. This format represents the 32 bit communities value, where AS is the high order 16 bits and VAL is the low order 16 bits in digit format.</td>
<td>Support 2 bytes AS number and 2 bytes community ID</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Do not advertise to any peer (well-known community).</td>
<td>-</td>
</tr>
<tr>
<td>no-export</td>
<td>Do not export to next AS (well-known community).</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

N/A

**Usage**

N/A

**Examples**

Switch# show bgp ipv6 community
Switch# show bgp ipv6 community.local-AS 100

**Related Commands**

N/A

**7.6.64 show bgp ipv6 community-list**

**Command Purpose**

Use this command to display routes that match the community-list.

**Command Syntax**

```
show ip bgp community-list LISTNAME ( exact-match | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISTNAME</td>
<td>Specifies the community list name.</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>exact-match</td>
<td>Displays only routes that have exactly the same specified communities.</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

N/A

**Usage**

N/A

**Examples**

Switch# show bgp ipv6 community-list mylist exact-match
Switch# show bgp ipv6 unicast community-list mylist
Related Commands
N/A

7.6.65 show bgp ipv6 dampening

Command Purpose
Use this command to display detailed information about dampening.

Command Syntax
show bgp ipv6 dampening ( dampened-paths | flap-statistics | parameters )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dampened-paths</td>
<td>Display paths suppressed due to dampening.</td>
<td>-</td>
</tr>
<tr>
<td>flap-statistics</td>
<td>Display flap statistics of routes.</td>
<td>-</td>
</tr>
<tr>
<td>parameters</td>
<td>Display details of configured dampening parameters.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
N/A

Usage
N/A

Examples
Enable bgp dampening to maintain dampened-path information in memory. The following is a sample output displaying all the dampening parameters:
Switch# show bgp ipv6 dampening parameters

Related Commands
N/A

7.6.66 show bgp ipv6 filter-list

Command Purpose
Use this command to display routes conforming to the filter-list.

Command Syntax
show ip bgp filter-list LISTNAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISTNAME</td>
<td>Specifies the access list name.</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
N/A

Usage
N/A
Examples

Switch# show bgp ipv6 filter-list mylist

Related Commands

N/A

7.6.67 show bgp ipv6 inconsistent-as

Command Purpose

Use this command to display routes with inconsistent AS Paths.

Command Syntax

show bgp ipv6 inconsistent-as

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

Switch# show bgp ipv6 inconsistent-as

Related Commands

N/A

7.6.68 show bgp ipv6 neighbors

Command Purpose

Use this command to display detailed information on TCP and BGP neighbor connections.

Command Syntax

show bgp ipv6 neighbors (IPV6_ADDR |)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPV6_ADDR</td>
<td>X:X::X:X Specifies the IPv6 address.</td>
<td>IPv6 Address</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

This is a sample output from the show bgp ipv6 neighbors command displaying information about the specified neighbor:
Switch# show bgp ipv6 neighbors
Related Commands
N/A

7.6.69  show bgp ipv6 paths

Command Purpose
Use this command to display BGP path information.

Command Syntax
show bgp ipv6 paths

Command Mode
Privileged EXEC

Default
N/A

Usage
N/A

Examples
Switch# show bgp ipv6 paths

Related Commands
N/A

7.6.70  show bgp ipv6 prefix-list

Command Purpose
Use this command to display routes matching the prefix-list.

Command Syntax
show bgp ipv6 prefix-list LIST

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIST</td>
<td>Specifies the name of the IPv6 prefix list.</td>
<td>Up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
N/A

Usage
N/A

Examples
Switch# show bgp ipv6 prefix-list mylist

Related Commands
N/A
7.6.71 show bgp ipv6 quote-regexp

Command Purpose
Use this command to display routes matching the AS path regular expression in quotes.

Command Syntax
show bgp ipv6 quote-regexp WORD

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>Specifies a regular-expression to match the BGP AS paths</td>
<td>Regular expression in quotes</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
N/A

Usage
N/A

Examples
Switch# show bgp ipv6 quote-regexp "Switch"

Related Commands
N/A

7.6.72 show bgp ipv6 regexp

Command Purpose
Use this command to display routes matching the AS path regular expression.

Command Syntax
show bgp ipv6 regexp LINE

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LINE</td>
<td>Displays routes matching the AS path regular expression.</td>
<td>Regular expression</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
N/A

Usage
N/A

Examples
Switch# show bgp ipv6 regexp myexpression

Related Commands
N/A
7.6.73  show bgp ipv6 summary

Command Purpose
Use this command to display a summary of BGP neighbor status.

Command Syntax
show bgp ipv6 summary

Command Mode
Privileged EXEC

Default
N/A

Usage
N/A

Examples
This is a sample output from the show bgp ipv6 summary command displaying a summary of BGP neighbor status:

```
Switch# show bgp ipv6 summary
```

Related Commands
N/A

7.6.74  timers

Command Purpose
Use this command sets the BGP keepalive timer and holdtime timer values.
Use the no parameter with this command to reset timers to default value.

Command Syntax
timers bgp KEEPALIVE HOLDTIME
do not timers bgp

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEEPALIVE</td>
<td>&lt;0-65535&gt; The frequency with which the keepalive messages are sent to the neighbors. The default value is 60 seconds.</td>
<td>0-65535</td>
</tr>
<tr>
<td>HOLDTIME</td>
<td>The interval after which the neighbor is considered dead if keepalive messages are not received. The default holdtime value is 180 seconds.</td>
<td>3-65535</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration

Default
N/A

Usage
This command is used globally to set or unset the keepalive and holdtime values for all the neighbors.

Examples
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# timers bgp 40 120

Related Commands
N/A
Chapter 8 Multicast Commands

8.1 IP Multicast-Routing Commands

8.1.1 ip multicast-routing

Command Purpose
Use this command to enable ip multicast routing. To disable ip multicast routing, use the no form of this command.

Command Syntax

ip multicast-routing
no ip multicast-routing

Command Mode
Global Configuration

Default
Enable

Usage
None

Examples

This example shows how to enable ip multicast routing:
Switch# configure terminal
Switch(config)# ip multicast-routing

This example shows how to disable ip multicast routing:
Switch# configure terminal
Switch(config)# no ip multicast-routing

Related Commands
None

8.1.2 ip multicast route-limit

Command Purpose
Use this command to set the maximum number of the multicast routes. To return it to default value, use the no form of this command.

Command Syntax

ip multicast route-limit ROUTE_NUMBER ( THRESHOLD_NUMBER | )
no ip multicast route-limit

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROUTE_NUMBER</td>
<td>Max number of multicast route entries</td>
<td>1-2048</td>
</tr>
<tr>
<td>THRESHOLD_NUMBER</td>
<td>Threshold at which to generate warning message</td>
<td>1-2048</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
Default maximum number of the multicast routes is 2048. Default threshold is same as the maximum number of multicast routes.
**Usage**
None

**Examples**
This example shows how to set the maximum number of the multicast routes to 512:
Switch# configure terminal
Switch(config)# ip multicast route-limit 512
This example shows how to return the maximum number of the multicast routes to default value:
Switch# configure terminal
Switch(config)# no ip multicast route-limit

**Related Commands**
show ip mroute route-limit

**8.1.3 show ip mroute**

**Command Purpose**
Use this command to display the ip multicast routing table information.

**Command Syntax**
show ip mroute (sparse |) (count | summary |)
s how ip mroute IP_ADDR (sparse |) (count | summary |)
show ip mroute route-limit

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>sparse</td>
<td>Show sparse multicast routes</td>
<td>-</td>
</tr>
<tr>
<td>count</td>
<td>Show number of multicast route entries</td>
<td>-</td>
</tr>
<tr>
<td>summary</td>
<td>Show abbreviated multicast route information</td>
<td>-</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>Show specify source or group address multicast route</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>route-limit</td>
<td>Show max route limit value</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
This example shows how to display multicast routing table:
Switch# show ip mroute

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(10.0.1.20, 228.1.1.1), uptime 00:35:46, stat expires 00:02:19
Owner PIM-SM, Flags: TF
   Incoming interface: eth-0-1
   Outgoing interface list:
      eth-0-2 (1)
This example shows how to display multicast routing table summary information:
Switch# show ip mroute summary

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expirey
Interface State: Interface (TTL)
(10.0.1.20, 228.1.1.1), 00:36:59/00:02:46, PIM-SM, Flags: TF

Related Commands

ip multicast route-limit
ip mrouting-rpf

8.1.4 show ip mvif

Command Purpose
Use this command to display the multicast interface information.

Command Syntax

show ip mvif (IFNAME )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display multicast interface information:
Switch# show ip mvif

<table>
<thead>
<tr>
<th>Interface</th>
<th>Vif</th>
<th>Owner</th>
<th>TTL</th>
<th>Local Address</th>
<th>Remote Address</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-0-1</td>
<td>0</td>
<td>PIM-SM</td>
<td>1</td>
<td>10.0.1.1</td>
<td>0.0.0.0</td>
<td>00:42:56</td>
</tr>
<tr>
<td>eth-0-2</td>
<td>2</td>
<td>PIM-SM</td>
<td>1</td>
<td>10.0.2.1</td>
<td>0.0.0.0</td>
<td>00:42:53</td>
</tr>
</tbody>
</table>

Related Commands

ip pim sparse-mode

8.1.5 show ip multicast groups count

Command Purpose

Use this command to display the multicast group count.

Command Syntax

show ip multicast groups count

Command Mode

Privileged EXEC

Default

None

Usage

None
Examples

This example shows how to display multicast group number:
Switch# show ip multicast groups count

<table>
<thead>
<tr>
<th>multicast group record count:</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast source record count:</td>
<td>0</td>
</tr>
<tr>
<td>multicast total record count:</td>
<td>1</td>
</tr>
<tr>
<td>multicast max record count:</td>
<td>2048</td>
</tr>
</tbody>
</table>

Related Commands

None

8.1.6 show resource mcast

Command Purpose

Use this command to display multicast resource information.

Command Syntax

show resource mcast

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display multicast resource information:
Switch# show resource mcast

<table>
<thead>
<tr>
<th>MCAST Resource</th>
<th>Used</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mcast Entry</td>
<td>0</td>
<td>1023</td>
</tr>
<tr>
<td>Mcast Normal Member</td>
<td>0</td>
<td>2046</td>
</tr>
<tr>
<td>Mcast Vlan Member</td>
<td>0</td>
<td>1023</td>
</tr>
</tbody>
</table>

Related Commands

None

8.1.7 clear ip mroute

Command Purpose

Use this command to clear the multicast routing table information.

Command Syntax

clear ip mroute (* | GRP_ADDR (SRC_IP) |)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRP_ADDR</td>
<td>Clear specify group address multicast route</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>SRC_ADDR</td>
<td>Clear specify source address multicast route</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>*</td>
<td>Clear all multicast routes</td>
<td>-</td>
</tr>
</tbody>
</table>

www.fs.com
**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

This example shows how to clear all multicast routing table information:

```bash
Switch# clear ip mroute *
```

**Related Commands**

`show ip mroute`

---

**8.2 IGMP Commands**

**8.2.1 ip igmp access-group**

**Command Purpose**

Use this command to apply an access-list to the igmp interface.
To remove this setting, use the no form of this command.

**Command Syntax**

```
ip igmp access-group LIST
no ip igmp access-group
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIST</td>
<td>The name of the ip access-list to be applied.</td>
<td>Up to 40 characters</td>
</tr>
<tr>
<td></td>
<td>The format of access-list should be ipv4.</td>
<td></td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

Access-group is not configured on any igmp interface by default.

**Usage**

No matter the source ip or the destination ip in ACE should take effect respectively. If ACE's action is deny, then the packet should be ignored; otherwise, if it matches one whose action is permit, then it should be processed regularly.

**Examples**

This example shows how to apply the access-list acl1 to the interface vlan1:

```bash
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp access-group acl1
```

This example shows how to remove the access-list acl1 on the interface:

```bash
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip igmp access-group
```

**Related Commands**

`show ip igmp interface`
8.2.2  ip igmp immediate-leave group-list

Command Purpose
Use this command to apply an access-list to configure which groups support immediate-leave per interface. To remove this setting, use the no form of this command.

Command Syntax
ip igmp immediate-leave group-list LIST
no ip igmp immediate-leave

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIST</td>
<td>The name of the ip access-list to be applied. The format of access-list should be ipv4.</td>
<td>Up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
Access-group is not configured on any igmp interface by default.

Usage
No matter the source ip or the destination ip in ACE should take effect respectively. If ACE's action is deny, then the packet should be ignored; Otherwise if it matches one whose action is permit, then it should be processed regularly.

Examples
This example shows how to apply an access-list to configure which groups support immediately-leave on interface vlan1:
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp immediate-leave group-list acl1
This example shows how to remove the access-list acl1 on the interface:
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip igmp immediate-leave group-list

Related Commands
show ip igmp interface

8.2.3  ip igmp last-member-query-count

Command Purpose
Use this command to set the value of last member query count. To reset it to default value, use the no form of this command.

Command Syntax
ip igmp last-member-query-count COUNT
no ip igmp last-member-query-count

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>COUNT</td>
<td>The value of last member query count</td>
<td>2-7</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
2
Usage
None

Examples
This example shows how to set the value of last member query count to 5:
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp last-member-query-count 5
This example shows how to reset the value of last member query count to default value:
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip igmp last-member-query-count

Related Commands
show ip igmp interface
ip igmp last-member-query-count

8.2.4 ip igmp last-member-query-interval

Command Purpose
Use this command to set the value of last member query interval. To reset it to default value, use the no form of this command.

Command Syntax
ip igmp last-member-query-interval INTERVAL
no ip igmp last-member-query-interval

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>The last member query interval value(ms)</td>
<td>1000-25500 ms</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
1000ms

Usage
None

Examples
This example shows how to set the last member query interval value to 10000ms:
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp last-member-query-interval 10000
This example shows how to reset the last member query interval value to default value:
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip igmp last-member-query-interval

Related Commands
show ip igmp interface
ip igmp last-member-query-count
8.2.5  ip igmp limit

Command Purpose
Use this command to set the max num of groups allowed. 
To reset it to default value, use the no form of this command.

Command Syntax
ip igmp limit NUMBER except LIST
no ip igmp limit

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>The max num of groups</td>
<td>1-2048</td>
</tr>
<tr>
<td>LIST</td>
<td>Groups not to be counted</td>
<td></td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration & Interface Configuration

Default
2048

Usage
Max number of groups is 2048 by default, in global configuration mode, use this command to set number of groups for all ports, in interface configuration mode, use this command to set number of groups for one ports

Examples
This example shows how to set the max num of groups allowed to 1000 globally:
Switch# configure terminal
Switch(config)# ip igmp limit 1000
This example shows how to reset the max num of groups to default value:
Switch# configure terminal
Switch(config)# no ip igmp limit

Related Commands
show ip igmp interface

8.2.6  ip igmp mroute-proxy

Command Purpose
Use this command to set the mroute-proxy port on this interface. 
To remove it, use the no form of this command.

Command Syntax
ip igmp mroute-proxy IFNAME
no ip igmp mroute-proxy

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>The interface name of the mroute-proxy port</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
None
Usage

This command is used to set the mroute-proxy port on the interface. Only one mroute-proxy port can be set on the interface. When set it again, the new setting will overwrite the old one.

Examples

This example shows how to set the mroute-proxy port to eth-0-1 on this interface:
```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp mroute-proxy eth-0-1
```

This example shows how to remove the mroute-proxy port on this interface:
```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip igmp mroute-proxy
```

Related Commands

ip igmp proxy-service

8.2.7 ip igmp proxy-service

Command Purpose

Use this command to enable igmp mroute proxy service on the interface. To disable it, use the no form of this command.

Command Syntax

```
ip igmp proxy-service
no ip igmp proxy-service
```

Command Mode

Interface Configuration

Default

None

Usage

This command is used with command ip igmp mroute-proxy and to set the upstream interface of the igmp group.

Examples

This example shows how to enable igmp mroute proxy service on this interface:
```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp mroute-proxy
```

This example shows how to disable igmp mroute proxy service:
```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip igmp mroute-proxy
```

Related Commands

ip igmp mroute-proxy

8.2.8 ip igmp querier-timeout

Command Purpose

Use this command to set the igmp previous querier timeout value. To reset it to default value, use the no form of this command.

Command Syntax

```
ip igmp querier-timeout INTERVAL
no ip igmp querier-timeout
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>The igmp previous querier timeout value</td>
<td>60-300 seconds</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

255s

**Usage**

None

**Examples**

This example shows how to set the igmp previous querier timeout value to 100 seconds:
```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp querier-timeout 100
```

This example shows how to reset the igmp previous querier timeout value to default value:
```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip igmp querier-timeout
```

**Related Commands**

- ip igmp query-interval
- ip igmp query-max-response-time

### 8.2.9 ip igmp query-interval

**Command Purpose**

Use this command to set the igmp query interval. To reset it to default value, use the no form of this command.

**Command Syntax**

```
ip igmp query-interval INTERVAL
no ip igmp query-interval
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>The value of igmp query interval</td>
<td>2-18000</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

125s

**Usage**

None

**Examples**

This example shows how to set the igmp query interval to 300 seconds:
```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp query-interval 300
```
This example shows how to reset the igmp query interval to default value:

Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip igmp query-interval

### Related Commands

- `ip igmp querier-timeout`
- `ip igmp query-max-response-time`

#### 8.2.10 ip igmp query-max-response-time

**Command Purpose**

Use this command to set the igmp query max response time. To reset it to default value, use the no form of this command.

**Command Syntax**

```
ip igmp query-max-response-time INTERVAL
no ip query-max-response-time
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>The igmp query max response time</td>
<td>1-25</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

10 seconds

**Usage**

Query max response time must be less than igmp query interval.

**Examples**

This example shows how to set the igmp query max response time to 20 seconds:

Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp query-max-response-time 20

This example shows how to reset the igmp query max response time to default value:

Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip igmp query-max-response-time

**Related Commands**

- `ip igmp querier-timeout`
- `ip igmp query-interval`

#### 8.2.11 ip igmp robustness-variable

**Command Purpose**

Use this command to set the igmp querier robustness variable value. To reset it to default value, use the no form of this command.

**Command Syntax**

```
ip igmp robustness-variable VALUE
no ip robustness-variable
```

**Examples**

This example shows how to set the igmp query max response time to 20 seconds:
### Command Mode

Interface Configuration

### Default

2

### Usage

None

### Examples

This example shows how to set the igmp querier robustness variable value to 6:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp robustness-variable 6
```

This example shows how to reset the igmp querier robustness variable value to default value:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip igmp robustness-variable
```

### Related Commands

show ip igmp interface

### 8.2.12 ip igmp version

#### Command Purpose

Use this command to set the igmp version on interface. To reset it to default value, use the no form of this command.

#### Command Syntax

```
ip igmp version VER
no ip igmp version
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VER</td>
<td>The igmp version on the interface</td>
<td>1-3</td>
</tr>
</tbody>
</table>

### Command Mode

Interface Configuration

### Default

2

### Usage

None

### Examples

This example shows how to set the igmp version 1 on the interface:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp version 1
```

This example shows how to reset the igmp version to default value:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip igmp version
```
### Related Commands

show ip igmp interface

### 8.2.13 ip igmp static-group

#### Command Purpose

Use this command to configure the static multicast group on interface. To delete static group, use the no form of this command.

#### Command Syntax

```
ip igmp static-group GRP_ADDR ( source SRC_ADDR | )
no ip igmp static-group GRP_ADDR ( source SRC_ADDR | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRP_ADDR</td>
<td>The multicast group address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>SRC_ADDR</td>
<td>The multicast source address</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

#### Command Mode

Interface Configuration

#### Default

None

#### Usage

None

#### Examples

This example shows how to configure the static IGMP group on interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ip igmp static-group 226.1.2.3
Switch(config-if)# ip igmp static-group 226.1.2.4 source 1.2.3.4
```

This example shows how to delete static igmp group on interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ip igmp static-group 226.1.2.3
```

#### Related Commands

show ip igmp groups

### 8.2.14 ip igmp ssm-map enable

#### Command Purpose

Use this command to enable igmp ssm mapping. To disable ssm mapping, use the no form of this command.

#### Command Syntax

```
ip igmp ssm-map enable
no ip igmp ssm-map enable
```

#### Command Mode

Global Configuration

#### Default

Disable
Usage

None

Examples

This example shows how to enable igmp ssm mapping:
Switch# configure terminal
Switch(config)# ip igmp ssm-map enable
This example shows how to disable igmp ssm mapping:
Switch# configure terminal
Switch(config)# no ip igmp ssm-map enable

Related Commands

None

8.2.15 ip igmp ssm-map static

Command Purpose

Use this command to set igmp ssm mapping. To cancel ssm mapping setting, use the no form of this command.

Command Syntax

ip igmp ssm-map static LIST SRC_ADDR
no ip igmp ssm-map static LIST SRC_ADDR

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIST</td>
<td>Specify multicast group address range access list</td>
<td>Up to 40 characters</td>
</tr>
<tr>
<td>SRC_ADDR</td>
<td>Multicast source address</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This example shows how to set igmp ssm mapping:
Switch# configure terminal
Switch(config)# ip igmp ssm-map static ipacl 192.168.1.1
This example shows how to unset igmp ssm mapping:
Switch# configure terminal
Switch(config)# no ip igmp ssm-map static ipacl 192.168.1.1

Related Commands

None

8.2.16 clear ip igmp

Command Purpose

Use this command to clear igmp groups.

Command Syntax

clear ip igmp group { * | GRP_ADDR }
### clear ip igmp group

#### Description
Clear igmp group.

#### Command Syntax
```
clear ip igmp group [GROUP_ADDR]
clear ip igmp group all
```

#### Parameter Table
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>All multicast group address</td>
<td>-</td>
</tr>
<tr>
<td>GRP_ADDR</td>
<td>Multicast group address</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

#### Command Mode
Privileged EXEC

#### Default
None

#### Usage
None

#### Examples
This example shows how to clear igmp group all:
```
Switch# clear ip igmp
```

This example shows how to clear igmp specified group:
```
Switch# clear ip igmp group 228.1.1.1
```

#### Related Commands
- show ip igmp groups

---

### clear ip igmp interface

#### Description
Clear igmp group on specified interface.

#### Command Syntax
```
clear ip igmp interface IFNAME
```

#### Parameter Table
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

#### Command Mode
Privileged EXEC

#### Default
None

#### Usage
None

#### Examples
This example shows how to clear igmp group on specified interface:
```
Switch# clear ip igmp group interface eth-0-1
```

#### Related Commands
- show ip igmp groups
8.2.18 show ip igmp groups

**Command Purpose**

Use this command to show the information about igmp groups.

**Command Syntax**

```
show ip igmp groups GRP_ADDR ( detail )
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRP_ADDR</td>
<td>Specify multicast group address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>detail</td>
<td>Detailed Information</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

This example shows how to display the detail information about igmp groups:

```
Switch# show ip igmp groups detail
```

```
Interface: eth-0-1
Group: 227.0.0.1
Uptime: 00:00:33
Group mode: Exclude (Expires: 00:04:18)
Last reporter: 10.0.1.100
Source list is empty
```

**Related Commands**

None

8.2.19 show ip igmp groups interface

**Command Purpose**

Use this command to show the information about igmp groups on interface.

**Command Syntax**

```
show ip igmp groups IFNAME ( GRP_ADDR | ) ( detail | )
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
<tr>
<td>GRP_ADDR</td>
<td>Specify multicast group address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>detail</td>
<td>Detailed Information</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC
Default
None

Usage
None

Examples
This example shows how to display the information about igmp groups on interface eth-0-1:

Switch# show ip igmp groups eth-0-1

IGMP Connected Group Membership

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Interface</th>
<th>Uptime</th>
<th>Expires</th>
<th>Last Reporter</th>
</tr>
</thead>
<tbody>
<tr>
<td>227.0.0.1</td>
<td>eth-0-1</td>
<td>00:01:11</td>
<td>00:04:16</td>
<td>10.0.1.100</td>
</tr>
</tbody>
</table>

Related Commands
None

8.2.20 show ip igmp groups count

Command Purpose
Use this command to show igmp group number.

Command Syntax
show ip igmp groups (IFNAME | ) count

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to display the igmp group number on interface eth-0-1:

Switch# show ip igmp groups eth-0-1 count

Dynamic multicast groups count: 1
Static multicast groups count: 0
Total multicast groups count: 1

Related Commands
None

8.2.21 show ip igmp interface

Command Purpose
Use this command to show the information about igmp on interface.
Command Syntax

show ip igmp interface ( IFNAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the information about igmp on interface eth-0-1:

Switch# show ip igmp interface eth-0-1

Interface eth-0-1 (Index 1)
IGMP Enabled, Active, Querier, Version 2 (default)
Internet address is 10.0.1.1
IGMP interface limit is 8192
IGMP interface has 1 group-record states
IGMP activity: 97 joins, 0 leaves
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1000 milliseconds
Group Membership interval is 260 seconds
Last memeber query count is 2
Robustness Variable is 2

Related Commands

None

8.3 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 | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

Enable
Usage

Igmp Snooping can be enabled globally and per vlan. By default, igmp snooping is enabled globally and per vlan.

Examples

This example shows how to enable igmp snooping:
Switch# configure terminal
Switch(config)# ip igmp snooping
This example shows how to disable igmp snooping:
Switch# configure terminal
Switch(config)# no ip igmp snooping
This example shows how to enable igmp snooping on vlan 10:
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 10
This example shows how to disable igmp snooping on vlan 10:
Switch# configure terminal
Switch(config)# no ip igmp snooping vlan 10

Related Commands

show ip igmp snooping

8.3.1 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

Disable

Usage

This command will override immediate-leave setting.

Examples

This example shows how to enable igmp snooping fast-leave:
Switch# configure terminal
Switch(config)# ip igmp snooping fast-leave
This example shows how to disable igmp snooping fast-leave:
Switch# configure terminal
Switch(config)# no ip igmp snooping fast-leave

Related Commands

show ip igmp snooping global

8.3.2 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>INTERVAL</td>
<td>The last member query interval</td>
<td>1000-25500 ms</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

1000 ms

Usage

Igmp last member query interval can be configured per vlan. The default is 1000ms and the range is 1000-25500ms.

Examples

This example shows how to set the last member query interval:
Switch# configure terminal
Switch(config)# ip igmp snooping last-member-query-interval 2000

This example shows how to reset the last member query interval to default value:
Switch# configure terminal
Switch(config)# no ip igmp snooping last-member-query-interval

Related Commands

show ip igmp snooping
show ip igmp snooping vlan

8.3.3 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>The IPv4 address of source address</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

0.0.0.0

Usage

Will use global configured source-address if vlan is not configured, otherwise, use source-address config from vlan.

Examples

This example shows how to set the global source address to 1.3.4.5:
Switch# configure terminal
Switch(config)# ip igmp snooping global source-address 1.3.4.5
This example shows how to reset the global source address to default value:
Switch# configure terminal
Switch(config)# no ip igmp snooping global source-address

Related Commands
show ip igmp snooping querier

8.3.4 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>NUMBER</td>
<td>The max member number of igmp snooping</td>
<td>1-2048</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
2048

Usage
None

Examples
This example shows how to set the max member number of igmp snooping to 1024:
Switch# configure terminal
Switch(config)# ip igmp snooping max-member-num 1024
This example shows how to reset the max member number to default value:
Switch# configure terminal
Switch(config)# no ip igmp snooping max-member-num

Related Commands
show ip igmp snooping global
show ip igmp snooping vlan

8.3.5 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>INTERVAL</td>
<td>The query-interval of igmp snooping</td>
<td>2-18000 seconds</td>
</tr>
</tbody>
</table>
Command Mode
Global Configuration

Default
125s

Usage
Query interval can not be less than igmp snooping query max response time.

Examples
This example shows how to set the igmp snooping query interval to 64s:
Switch# configure terminal
Switch(config)# ip igmp snooping query-interval 64
This example shows how to reset the query-interval to default value:
Switch# configure terminal
Switch(config)# no ip igmp snooping query-interval

Related Commands
show ip igmp snooping querier
show ip igmp snooping querier vlan

8.3.6 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>TIME</td>
<td>The query max response time in seconds</td>
<td>1-25</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
10s

Usage
Query interval can not be less than igmp snooping query max response time.

Examples
This example shows how to set the igmp snooping query max response time to 15s:
Switch# configure terminal
Switch(config)# ip igmp snooping query-max-response-time 15
This example shows how to reset the query max response time to default value:
Switch# configure terminal
Switch(config)# no ip igmp snooping query-max-response-time

Related Commands
show ip igmp snooping querier
show ip igmp snooping querier vlan
8.3.7 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**

```plaintext
ip igmp snooping { vlan VLAN_ID | } report-suppression
no ip igmp snooping { vlan VLAN_ID | } report-suppression
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

**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:

```plaintext
Switch# configure terminal
Switch(config)# ip igmp snooping report-suppression
```

This example shows how to disable report suppression:

```plaintext
Switch# configure terminal
Switch(config)# no ip igmp snooping report-suppression
```

**Related Commands**

- show ip igmp snooping
- show ip igmp snooping vlan

8.3.8 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**

```plaintext
ip igmp snooping { vlan VLAN_ID | } version VER
no ip igmp snooping { vlan VLAN_ID | } version
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>VER</td>
<td>Igmp snooping version</td>
<td>1-3</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

2

**Usage**

The default version is 2.
Examples

This example shows how to set the igmp snooping version 1:

Switch# configure terminal
Switch(config)# ip igmp snooping version 1

Related Commands

show ip igmp snooping
show ip igmp snooping vlan

8.3.9 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

Enabled by default, unknown multicast traffic will flood in vlan.

Usage

None

Examples

This example shows how to enable discard-unknown multicast traffic:

Switch# configure terminal
Switch(config)# ip igmp snooping discard-unknown

Related Commands

show ip igmp snooping
show ip igmp snooping vlan

8.3.10 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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>IGMP querier TCN query enable</td>
<td>-</td>
</tr>
<tr>
<td>COUNT</td>
<td>IGMP querier TCN query count, default is 2.</td>
<td>1-10</td>
</tr>
<tr>
<td>INTERVAL</td>
<td>IGMP querier TCN query interval, default is 10s.</td>
<td>1-255 seconds</td>
</tr>
<tr>
<td>TIME</td>
<td>IGMP querier TCN query max response time, default is 5s</td>
<td>1-9 seconds</td>
</tr>
</tbody>
</table>
**Command Mode**
Global Configuration

**Default**
This feature is enabled by default, default query count is 2, default query interval is 10s, maximum response time is 5s

**Usage**
None

**Examples**
This example shows how to use ip igmp snooping querier tcn command:
```
Switch# configure terminal
Switch(config)# ip igmp snooping querier tcn query-count 2
```

**Related Commands**
show ip igmp snooping querier

---

**8.3.11  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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>LIST</td>
<td>IP Named Standard Access list.</td>
<td>Up to 40 characters</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
None

**Usage**
None

**Examples**
This example shows how to apply access-group on vlan 10:
```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 10 access-group acl
```
This example shows how to remove access-group from vlan 10:
```
Switch# configure terminal
Switch(config)# no ip igmp snooping vlan 10 access-group
```

**Related Commands**
show ip igmp snooping vlan

---

**8.3.12  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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Mrouter interface on this vlan</td>
<td>Support physical/aggregation ports</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

The specified interface must have already joined the configured vlan.

Examples

This example shows how to set eth-0-1 as mrouter interface on vlan 10:
```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 10 mrouter interface eth-0-1
```
This example shows how to unset eth-0-1 as mrouter interface on vlan 10:
```
Switch# configure terminal
Switch(config)# no ip igmp snooping vlan 10 mrouter interface eth-0-1
```

Related Commands

show ip igmp snooping vlan

8.3.13 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>INTERVAL</td>
<td>Dynamic mrouter interface aging interval on this vlan in seconds</td>
<td>1-65535 seconds</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

255s

Usage

None

Examples

This example shows how to set dynamic mrouter interface aging interval as 100 seconds on vlan 10:
```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 10 mrouter-aging-interval 100
```
This example shows how to reset dynamic mrouter interface aging interval as default on vlan 10:
Switch# configure terminal
Switch(config)# no ip igmp snooping vlan 10 mrouter-aging-interval

Related Commands

show ip igmp snooping vlan

8.3.14 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

Disable

Usage

None

Examples

This example shows how to enable querier on vlan 10:
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 10 querier
This example shows how to disable querier on vlan 10:
Switch# configure terminal
Switch(config)# no ip igmp snooping vlan 10 querier

Related Commands

show ip igmp snooping querier vlan

8.3.15 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>The address of querier on this vlan</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>
Default
None

Usage
Will use global configured source-address if vlan is not configured, otherwise, use source-address config from vlan.

Examples
This example shows how to set querier address on vlan 10:
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 10 querier address 1.1.1.1
This example shows how to unset querier address on vlan 10:
Switch# configure terminal
Switch(config)# no ip igmp snooping vlan 10 querier address

Related Commands
show ip igmp snooping querier vlan

8.3.16 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>INTERVAL</td>
<td>The igmp previous querier timeout interval on this vlan in</td>
<td>60-300 seconds</td>
</tr>
<tr>
<td></td>
<td>seconds</td>
<td></td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
255s

Usage
None

Examples
This example shows how to set previous querier timeout interval as 100 seconds on vlan 10:
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 10 querier-timeout 100
This example shows how to reset previous querier timeout interval on vlan 10:
Switch# configure terminal
Switch(config)# no ip igmp snooping vlan 10 querier-timeout

Related Commands
show ip igmp snooping querier vlan
8.3.17 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>GRP_ADDR</td>
<td>The address of group configured on the specified interface.</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>SRC_ADDR</td>
<td>The address of source configured on the specified interface.</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IFNAME</td>
<td>The interface configured as a member of specified group on this vlan</td>
<td>Support physical/aggregation ports</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default
None

Usage
None

Examples

This example shows how to add group 238.1.1.1 on interface eth-0-11 of vlan 10:
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 10 static-group 238.1.1.1 interface eth-0-11

This example shows how to remove group 238.1.1.1 from interface eth-0-11 of vlan 10:
Switch# configure terminal
Switch(config)# no ip igmp snooping vlan 10 static-group 238.1.1.1 interface eth-0-11

Related Commands
show ip igmp snooping group

8.3.18 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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>All multicast group address</td>
<td>-</td>
</tr>
<tr>
<td>GRP_ADDR</td>
<td>Multicast group address</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC
Default
None

Usage
None

Examples
This example shows how to clear igmp snooping group all:
Switch# clear ip igmp snooping group *

Related Commands
None

8.3.19 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to clear igmp snooping group on vlan 10:
Switch# clear ip igmp snooping vlan 10

Related Commands
None

8.3.20 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

<table>
<thead>
<tr>
<th>Global Igmp Snooping Configuration</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Igmp Snooping</td>
<td>:Enabled</td>
</tr>
<tr>
<td>Igmp Snooping Fast-Leave</td>
<td>:Disabled</td>
</tr>
<tr>
<td>Igmp Snooping Version</td>
<td>:2</td>
</tr>
<tr>
<td>Igmp Snooping Robustness Variable</td>
<td>:2</td>
</tr>
<tr>
<td>Igmp Snooping Max-Member-Number</td>
<td>:2048</td>
</tr>
<tr>
<td>Igmp Snooping Unknown Multicast Behavior</td>
<td>:Flood</td>
</tr>
<tr>
<td>Igmp Snooping Report-Suppression</td>
<td>:Enabled</td>
</tr>
</tbody>
</table>

Related Commands
None

8.3.21 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

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Interface</th>
<th>Group-Address</th>
<th>Uptime</th>
<th>Expires-time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>eth-0-1</td>
<td>227.0.0.1</td>
<td>00:03:44</td>
<td>00:04:18</td>
</tr>
</tbody>
</table>

Related Commands
None

8.3.22 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 | )
### Command Mode

Privileged EXEC

### Default

None

### Usage

None

### Examples

This example shows how to display igmp snooping groups on vlan 1:
```
Switch# show ip igmp snooping groups vlan 1
```
IGMP Snooping groups for vlan1  
Interface: eth-0-1  
Group: 227.0.0.1  
Uptime: 00:05:24  
Group mode: Exclude (Expires: 00:04:20)  
Last reporter: 10.0.1.100  
Source list is empty

### Related Commands

None

#### 8.3.23 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

### 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

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>GRP_ADDR</td>
<td>The address of group</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>
**Related Commands**

None

**8.3.24 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 |)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

This example shows how to display the configurations of igmp snooping querier on vlan 1:

```
Switch# show ip igmp snooping querier vlan 1
```

Global Igmp Snooping Querier Configuration

```
Version :2  
Last-Member-Query-Interval (msec) :1000  
Last-Member-Query-Count :2  
Max-Query-Response-Time (sec) :10  
Query-Interval (sec) :125  
Global Source-Address :0.0.0.0  
TCN Query Count :2  
TCN Query Interval (sec) :10  
TCN Query Max Response Time (sec) :5  
Vlan 1 : IGMP snooping querier status
```

Elected querier is : 0.0.0.0

```
Admin state :Disabled  
Admin version :2  
Operational state :Non-Querier  
querier operational address :0.0.0.0  
querier configure address :N/A  
Last-Member-Query-Interval (msec) :1000  
Last-Member-Query-Count :2  
Max-Query-Response-Time (sec) :10  
Query-Interval (sec) :125  
Querier-Timeout (sec) :255
```

**Related Commands**

None
8.3.25 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 | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Mode</th>
<th>Uptime</th>
<th>Expires-time</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-0-11</td>
<td>static</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Related Commands

None

8.3.26 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 | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

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 Unknown Multicast Behavior** | :Flood
---
**Igmp Snooping Group Access-list** | : N/A
---
**Igmp Snooping Mrouter Port** | :
---
**Igmp Snooping Mrouter Port Aging Interval(sec)** | :255
---

**Related Commands**

None

**8.3.27 show resource l2mcast**

**Command Purpose**

Use this command to display the resource usage of L2 multicast.

**Command Syntax**

`show resource l2mcast`

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

The following is sample output from the show resource l2mcast command:

```
Switch# show resource l2mcast
L2MCAST
Resource Used Capability
-------------------------------------------------------------
L2 Mcast Entry 0 2048
```

**Related Commands**

None

**8.4 PIM Commands**

**8.4.1 ip pim accept-register**

**Command Purpose**

Use this command to apply an access-list to limit the pim register message received by rp.
To remove this setting, use the no form of this command.
**Command Syntax**

`ip pim accept-register list LIST`
`no ip pim accept-register`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIST</td>
<td>The name of the access-list to be applied.</td>
<td>Up to 40 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

None

**Usage**

This feature is used to prevent the unauthorized user registered to the switch.
When enable this feature, the system will send back a register stop message when the unauthorized register message is received.

**Examples**

This example shows how to apply the access-list acl1 to limit the pim register message received by rp:
```
Switch# configure terminal
Switch(config)# ip pim accept-register list acl1
```
This example shows how to remove the limits:
```
Switch# configure terminal
Switch(config)# no ip pim accept-register
```

**Related Commands**

None

---

**8.4.2 ip pim anycast-rp**

**Command Purpose**

Use this command to set anycast rendezvous-point.
To remove the configurations, use the no form of this command.

**Command Syntax**

`ip pim anycast-rp ANYCAST_RP_ADDR ANYCAST_MEMBER_ADDR`
`no ip pim anycast-rp ANYCAST_RP_ADDR (ANYCAST_MEMBER_ADDR)`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANYCAST_RP_ADDR</td>
<td>Anycast rp address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>ANYCAST_MEMBER_ADDR</td>
<td>Anycast member rp address</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

None.

**Usage**

Should configure every router in the network, and must configure same RP address.

**Examples**

This example shows how to set anycast rendezvous-point:
```
Switch# configure terminal
Switch(config)# ip pim anycast-rp 10.10.10.1 10.10.10.11
```
This example shows how to remove the member in anycast rendezvous-point:
Switch# configure terminal
Switch(config)# no ip pim anycast-rp 10.10.10.1 10.10.10.11

Related Commands
None

8.4.3 ip pim bsr-candidate

Command Purpose
Use this command to configure the candidate bootstrap router (candidate BSR). To remove the configurations, use the no form of this command.

Command Syntax
ip pim bsr-candidate IFNAME ( MASK _ LEN ( PRIORITY ) | )
no ip pim bsr-candidate

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
<tr>
<td>MASK _ LEN</td>
<td>Hash mask length for RP selection</td>
<td>0-32</td>
</tr>
<tr>
<td>PRIORITY</td>
<td>Priority value for candidate bootstrap router</td>
<td>0-255</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
None

Examples
This example shows how to configure the candidate BSR:
Switch# configure terminal
Switch(config)# ip pim bsr-candidate eth-0-1
This example shows how to cancel the candidate BSR configured:
Switch# configure terminal
Switch(config)# no ip pim bsr-candidate

Related Commands
ip pim bsr-border

8.4.4 ip pim bsr-border

Command Purpose
Use this command to configure the border of pim domain. To remove the configurations of the border of pim domain, use the no form of this command.

Command Syntax
ip pim bsr-border
no ip pim bsr-border

Command Mode
Interface Configuration
**8.4.5 ip pim dr-priority**

**Command Purpose**
Use this command to configure DR priority. To reset it to default value, use the no form of this command.

**Command Syntax**

```
ip pim dr-priority PRIORITY
no ip pim dr-priority
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRIORITY</td>
<td>The DR priority</td>
<td>0-4294967294</td>
</tr>
</tbody>
</table>

**Command Mode**
Interface Configuration

**Default**
1

**Usage**
When a hello message without DR priority is received, it will be regarded to have the max DR priority and to be elected as DR. When more than one router's hello messages do not have DR priority, the one which have the highest ip address will be elected as DR.

**Examples**
This example shows how to set the pim router DR priority to 1000:
```
Switch# configure terminal
Switch(config-if)# ip pim dr-priority 1000
```
This example shows how to reset the pim router DR priority to default value:
```
Switch# configure terminal
Switch(config-if)# no ip pim dr-priority
```

**Related Commands**

None

**8.4.6 ip pim exclude-genid**

**Command Purpose**
Use this command to exclude generation id option from pim hello packets on this interface. To reset to the default setting, use the no form of this command.
**Command Syntax**

ip pim exclude-genid
no ip pim exclude-genid

**Command Mode**

Interface Configuration

**Default**

Disable

**Usage**

GenerationID is the ID of a PIM neighbour, it is carried in PIM hello message, the receiver device will record every received GenerationID in the hello packet and check if GenerationID has changed, if GenerationID changed, will consider neighbour state changed and restart state machine.

**Examples**

This example shows how to exclude generation id option from pim hello packets on this interface:

```
Switch# configure terminal
Switch(config-if)# ip pim exclude-genid
```

This example shows how to reset the generation id option to the default setting:

```
Switch# configure terminal
Switch(config-if)# no ip pim exclude-genid
```

**Related Commands**

None

8.4.7 ip pim hello-interval

**Command Purpose**

Use this command to configure the interval for pim hello packets on this interface.

To reset to the default setting, use the no form of this command.

**Command Syntax**

ip pim hello-interval INTERVAL
no ip pim hello-interval

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>The pim hello message interval in second</td>
<td>1-18724</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

30s

**Usage**

None

**Examples**

This example shows how to set the pim hello message interval to 100s:

```
Switch# configure terminal
Switch(config-if)# ip pim hello-interval 100
```

This example shows how to reset the pim hello message interval to default value:

```
Switch# configure terminal
Switch(config-if)# no ip pim hello-interval
```
Related Commands

None

8.4.8 ip pim ignore-rp-set-priority

Command Purpose

Use this command to ignore RP set priority value.
To not ignore the priority, use the no form of this command.

Command Syntax

ip pim ignore-rp-set-priority
no ip pim ignore-rp-set-priority

Command Mode

Global Configuration

Default

Not ignore RP set priority value.

Usage

None

Examples

This example shows how to ignore RP set priority value:
Switch# configure terminal
Switch(config)# ip pim ignore-rp-set-priority
This example shows how to reset the configurations to default value:
Switch# configure terminal
Switch(config)# no ip pim ignore-rp-set-priority

Related Commands

None

8.4.9 ip pim jp-timer

Command Purpose

Use this command to set the join/prune timer value.
To reset the timer to default value, use the no form of this command.

Command Syntax

ip pim jp-timer TIMER
no ip pim jp-timer

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIMER</td>
<td>The Join/Prune timer (second)</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

60s

Usage

None
Examples

This example shows how to set the join/prune timer value to 100s:
Switch# configure terminal
Switch(config)# ip pim jp-timer 100
This example shows how to reset the join/prune timer value to default value:
Switch# configure terminal
Switch(config)# no ip pim jp-timer

Related Commands

None

8.4.10  ip pim neighbor-filter

Command Purpose

Use this command to add an access-list to filter the neighbor.
To remove this filter, use the no form of this command.

Command Syntax

ip pim neighbor-filter LIST
no ip pim neighbor-filter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIST</td>
<td>The name of the access-list</td>
<td>Up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

None

Usage

Neighbours would send hello message to each other to establish connections with other neighbour, you can use this command to filter which neighbour can be connected or not.

Examples

This example shows how to establish neighbors based on access-list acl1:
Switch# configure terminal
Switch(config-if)# ip pim neighbor-filter acl1
This example shows how to cancel the filter:
Switch# configure terminal
Switch(config-if)# no ip pim neighbor-filter

Related Commands

None

8.4.11  ip pim register-rate-limit

Command Purpose

Use this command to set the rate limit for pim registers.
To reset the rate limit to default value, use the no form of this command.

Command Syntax

ip pim register-rate-limit LIMIT
no ip pim register-rate-limit
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIMIT</td>
<td>The rate limit for pim registers send from dr to rp</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

By default, will not limit PIM register messages, if a limit is set, PIM register messages will be discard when packet reached by this limit.

**Usage**

There is no rate limit for pim registers by default.
When the rate limit is configured, the exceed pim register message will be dropped on the rp.

**Examples**

This example shows how to set the rate limit for pim registers to 100 per second:
```
Switch# configure terminal
Switch(config)# ip pim register-rate-limit 100
```
This example shows how to cancel the rate limit:
```
Switch# configure terminal
Switch(config)# no ip pim register-rate-limit
```

**Related Commands**

ip pim register-rp-reachability
ip pim register-source
ip pim register-suppression

8.4.12 ip pim register-source

**Command Purpose**

Use this command to set the source address for pim register.
To reset the source address for pim register to default value, use the no form of this command.

**Command Syntax**

```
ip pim register-source IFNAME
no ip pim register-source
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>The name of the interface. Use the address of this interface to be the source address for pim register</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

The source address for pim register is the interface ip of dr by default.

**Usage**

None

**Examples**

This example shows how to set the source address for pim register to the ip address of interface eth-0-1:
```
Switch# configure terminal
Switch(config)# ip pim register-source eth-0-1
```
This example shows how to reset the source address for pim register to default value:
```
Switch# configure terminal
Switch(config)# no ip pim register-source
```
Related Commands

- ip pim register-rate-limit
- ip pim register-rp-reachability
- ip pim register-suppression

8.4.13 ip pim register-rp-reachability

Command Purpose

Use this command to enable rp reachability check for pim registers.
To disable this check, use the no form of this command.

Command Syntax

- ip pim register-rp-reachability
- no ip pim register-rp-reachability

Command Mode

Global Configuration

Default

Disable.

Usage

None

Examples

This example shows how to enable rp reachability check for pim registers:
Switch# configure terminal
Switch(config)#ip pim register-rp-reachability
This example shows how to disable rp reachability check for pim registers:
Switch# configure terminal
Switch(config)#no ip pim register-rp-reachability

Related Commands

- ip pim register-rate-limit
- ip pim register-source
- ip pim register-suppression

8.4.14 ip pim register-suppression

Command Purpose

Use this command to set the register suppression time.
To reset this time to default value, use the no form of this command.

Command Syntax

- ip pim register-suppression TIME
- no ip pim register-suppression

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIME</td>
<td>The register suppression time in seconds</td>
<td>11-18000 seconds</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

60s
Usage
None

Examples
This example shows how to set the register suppression time to 100s:
Switch# configure terminal
Switch(config)# ip pim register-suppression 100
This example shows how to reset the register suppression time to default value:
Switch# configure terminal
Switch(config)# no ip pim register-suppression

Related Commands
ip pim register-rate-limit
ip pim register-rp-reachability
ip pim register-source

8.4.15 ip pim rp-address

Command Purpose
Use this command to set the pim rp (rendezvous point) address. To remove this setting, use the no form of this command.

Command Syntax
ip pim rp-address IP_ADDR (LIST | override | )
no ip pim rp-address IP_ADDR {LIST | }

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>The rp address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>LIST</td>
<td>The name of an access-list</td>
<td>Up to 40 characters</td>
</tr>
<tr>
<td>override</td>
<td>Overrides dynamically learned RP mappings</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
None

Examples
This example shows how to set the pim rp address to 1.1.1.1:
Switch# configure terminal
Switch(config)# ip pim rp-address 1.1.1.1
This example shows how to remove the rp address 1.1.1.1:
Switch# configure terminal
Switch(config)# no ip pim rp-address 1.1.1.1

Related Commands
ip pim rp-candidate
ip pim rp-register-kat

8.4.16 ip pim rp-candidate

Command Purpose
Use this command to set the candidate rp. To remove the candidate rp, use the no form of this command.
Command Syntax

```
ip pim rp-candidate IFNAME { ( priority PRIORITY | interval INTERVAL | group-list LIST) }  
no ip pim rp-candidate { IFNAME }  
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>The name of the interface to be the candidate rp</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
<tr>
<td>PRIORITY</td>
<td>The Candidate-RP priority</td>
<td>0-255</td>
</tr>
<tr>
<td>INTERVAL</td>
<td>The C-RP advertisement interval in seconds</td>
<td>1-16383 seconds</td>
</tr>
<tr>
<td>LIST</td>
<td>Group ranges for this C-RP, only permit filters would be cared</td>
<td>Up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This example shows how to set the interface eth-0-1 to be the candidate rp:
```
Switch# configure terminal
Switch(config)# ip pim rp-candidate eth-0-1
```

This example shows how to cancel the configured candidate rp:
```
Switch# configure terminal
Switch(config)# no ip pim rp-candidate eth-0-1
```

Related Commands

ip pim rp-address

8.4.17 ip pim rp-register-kat

Command Purpose

Use this command to set the keepalive timer (KAT) for (S,G) at RP from PIM registers.
To reset this timer to default value, use the no form of this command.

Command Syntax

```
ip pim rp-register-kat TIME  
o no pim rp-register-kat  
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIME</td>
<td>The KAT time in seconds</td>
<td>1-65535 seconds</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

The register message send from dr will add an entry on rp. This entry will be aged when the keepalive timer expired which can be configured by this command.
Examples

This example shows how to set the keepalive timer to 100s at RP from PIM registers:
Switch# configure terminal
Switch(config)# ip pim rp-register-kat 100
This example shows how to reset this timer to default value:
Switch# configure terminal
Switch(config)# no ip pim rp-register-kat

Related Commands
ip pim rp-address
ip pim rp-candidate

8.4.18 ip pim spt-switch-threshold infinity

Command Purpose
Use this command to set the spt switch threshold to infinity.
To cancel this setting, use the no form of this command.

Command Syntax
ip pim spt-switch-threshold infinity (group-list LIST | )
no ip pim spt-switch-threshold infinity (group-list LIST | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIST</td>
<td>Group address access list</td>
<td>Up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
The DR will switch to spt immediately when received the first multicast packet by default.

Usage
None

Examples

This example shows how to set the spt switch threshold to infinity:
Switch# configure terminal
Switch(config)# ip pim spt-switch-threshold infinity
This example shows how to reset the spt-switch-threshold to default:
Switch# configure terminal
Switch(config)# no ip pim spt-switch-threshold infinity

Related Commands
show ip pim sparse-mode spt-threshold

8.4.19 ip pim cisco-register-checksum

Command Purpose
Use this command to calculate register checksum over whole packet (cisco compatibility).
To remove this setting, use the no form of this command.

Command Syntax
ip pim cisco-register-checksum (group-list LIST | )
no ip pim cisco-register-checksum (group-list LIST | )
### LIST

**Parameter** Group address access list  
**Parameter Value** Strings up to 40 characters

**Command Mode**

Global Configuration

**Default**

The register checksum defined in RFC is used by default.

**Usage**

The register checksum defined in RFC is used by default, if group-list is configured, only packets that verified can be sent in CISCO way.

**Examples**

This example shows how to set to calculate register checksum over whole packet:

```
Switch# configure terminal
Switch(config)# ip pim cisco-register-checksum
```

This example shows how to remove this setting:

```
Switch# configure terminal
Switch(config)# no ip pim cisco-register-checksum
```

**Related Commands**

None

### 8.4.20 ip pim sparse-mode

**Command Purpose**

Use this command to enable pim sparse mode on the interface.  
To disable pim sparse mode, use the no form of this command.

**Command Syntax**

```
ip pim sparse-mode ( passive | )
no ip pim sparse-mode ( passive | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>passive</td>
<td>Pim passive mode (local members only)</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

Disable

**Usage**

The pim hello message will not be sent out from the interface when the passive mode is configured.

**Examples**

This example shows how to enable pim sparse mode on the interface:

```
Switch# configure terminal
Switch(config-if)# ip pim sparse-mode
```

This example shows how to disable pim sparse mode on the interface:

```
Switch# configure terminal
Switch(config-if)# no ip pim sparse-mode
```

This example shows how to enable pim sparse mode passive on the interface:

```
Switch# configure terminal
Switch(config-if)# ip pim sparse-mode passive
```

**Related Commands**

None
8.4.21 ip pim dense-mode

Command Purpose

Use this command to enable pim dense mode on the interface. To disable pim dense mode, use the no form of this command.

Command Syntax

ip pim dense-mode (passive | )
no ip pim dense-mode

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>passive</td>
<td>Pim passive mode (local members only)</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

Disable

Usage

Pim sparse-mode and dense-mode can not take effect on the same interface. The pim hello message will not be sent out from the interface when the passive mode is configured.

Examples

This example shows how to enable pim dense mode on the interface:
Switch# configure terminal
Switch(config-if)# ip pim dense-mode
This example shows how to disable pim dense mode on the interface:
Switch# configure terminal
Switch(config-if)# no ip pim dense-mode
This example shows how to enable pim dense mode passive on the interface:
Switch# configure terminal
Switch(config-if)# ip pim dense-mode passive

Related Commands

None

8.4.22 ip pim propagation-delay

Command Purpose

Use this command to set propagation delay on its LAN. To cancel this setting, use the no form of this command.

Command Syntax

ip pim propagation-delay timer
no ip pim propagation-delay

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>timer</td>
<td>Propagation delay value</td>
<td>100-5000 ms</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

1000ms
Usage

If all routers on a LAN support the LAN Prune Delay option, then the PIM routers on that LAN will use the values received to adjust their J/P_OVERRIDE_INTERVAL on that interface and the interface is LAN Delay Enabled.

Examples

This example shows how to set propagation delay:
```
Switch# configure terminal
Switch(config-if)# ip pim propagation-delay 400
```
This example shows how to unset this setting:
```
Switch# configure terminal
Switch(config-if)# no ip pim propagation-delay
```

Related Commands

None

8.4.23 ip pim state-refresh origination-interval

Command Purpose

Use this command to set the interval of originator sending state refresh messages. To cancel this setting, use the no form of this command.

Command Syntax

```
ip pim state-refresh origination-interval INTERVAL
no ip pim state-refresh origination-interval
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>state-refresh origination-interval</td>
<td>1-100 seconds</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

60s

Usage

State Refresh Messages are generated periodically by the PIM-DM router directly connected to a source. This command can control the interval of two messages.

Examples

This example shows how to set state-refresh origination-interval:
```
Switch# configure terminal
Switch(config-if)# ip pim state-refresh origination-interval 50
```
This example shows how to unset this setting:
```
Switch# configure terminal
Switch(config-if)# no ip pim state-refresh origination-interval
```

Related Commands

None

8.4.24 ip pim unicast-bsm

Command Purpose

Use this command to enable sending and receiving of unicast BSM for backward compatibility. To cancel this setting, use the no form of this command.

Command Syntax

```
ip pim unicast-bsm
```
no ip pim unicast-bsm

**Command Mode**

Interface Configuration

**Default**

Disable

**Usage**

Interface will send BSM message to the whole pim domain by default.

**Examples**

This example shows how to enable sending and receiving of unicast BSM for backward compatibility:

```
Switch# configure terminal
Switch(config-if)# ip pim unicast-bsm
```

This example shows how to cancel this setting:

```
Switch# configure terminal
Switch(config-if)# no ip pim unicast-bsm
```

**Related Commands**

None

### 8.4.25 ip pim ssm

**Command Purpose**

Use this command to enable pim-ssm and set ssm group range. To cancel this setting, use the no form of this command.

**Command Syntax**

```
ip pim ssm (default | range LIST)
noc ip pim ssm
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Use 232.0.0.0/8 group range for SSM</td>
<td>-</td>
</tr>
<tr>
<td>LIST</td>
<td>ACL for group range to be used for SSM</td>
<td>Up to 40 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

Disable

**Usage**

None

**Examples**

This example shows how to enable pim-ssm and set ssm group range to default:

```
Switch# configure terminal
Switch(config-if)# ip pim ssm default
```

This example shows how to cancel this setting:

```
Switch# configure terminal
Switch(config-if)# no ip pim ssm default
```

**Related Commands**

None
8.4.26 show ip pim sparse-mode bsr-router

Command Purpose
Use this command to show the information of bootstrap router.

Command Syntax
show ip pim sparse-mode bsr-router

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to display the information of bootstrap router:
Switch# show ip pim sparse-mode bsr-router

PIMv2 bootstrap information
This system is the bootstrap router (BSR)
   BSR address: 12.0.9.2
   Uptime: 00:00:08, BSR Priority: 64, Hash mask length: 10
   Next bootstrap message in 00:00:04
   Role: Candidate BSR
   State: Elected BSR
   Candidate RP: 12.0.9.2(eth-0-9)
   Advertisement interval 60 seconds
   Next C-RP advertisement in 00:00:57

Related Commands
None

8.4.27 show ip pim sparse-mode interface

Command Purpose
Use this command to show the information of pim interface.

Command Syntax
show ip pim sparse-mode interface ( detail | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Detailed interface information</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None
Examples

This example shows how to display the information of pim interface:
Switch# show ip pim sparse-mode interface detail

eth-0-9 (vif 0):
Address 12.0.9.1, DR 12.0.9.2
Hello period 30 seconds, Next Hello in 26 seconds
Triggered Hello period 5 seconds
Neighbors:
12.0.9.2

Related Commands

None

8.4.28 show ip pim sparse-mode local-member

Command Purpose

Use this command to show the pim local membership information.

Command Syntax

show ip pim sparse-mode local-member (IFNAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display pim local membership information:
Switch# show ip pim sparse-mode local-members

PIM local membership information
eth-0-3:
  (*, 229.1.1.1) : Include
eth-0-9:
  (*, 228.1.1.1) : Include

Related Commands

None

8.4.29 show ip pim sparse-mode mroute

Command Purpose

Use this command to show the mroute information of pim sparse mode.

Command Syntax

show ip pim sparse-mode mroute (SRC_ADDR | GRP_ADDR | ) (detail | )
### Command Mode

Privileged EXEC

### Default

None

### Usage

None

### Examples

This example shows how to display pim mroute information:

```
Switch# show ip pim sparse-mode mroute detail
```

**IP Multicast Routing Table**

- 

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRC_ADDR</td>
<td>Source address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>GRP_ADDR</td>
<td>Group address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>detail</td>
<td>Detailed interface information</td>
<td>-</td>
</tr>
</tbody>
</table>

```
(*,*,RP) Entries: 0
(*,G) Entries: 2
(S,G) Entries: 0
(S,G rpt) Entries: 0
FCR Entries: 0

(*, 228.1.1.1) Uptime: 00:09:55
RP: 0.0.0.0, RPF nbr: None, RPF idx: None
Upstream:
State: NOT JOINED, SPT Switch: Enabled, JT: off
Downstream:
eth-0-9:
State: NO INFO, ET: off, PPT: off
Assert State: NO INFO, AT: off
Winner: 0.0.0.0, Metric: 4294967295, Pref: 4294967295, RPT bit: on
Local Olist:
eth-0-9

(*, 229.1.1.1) Uptime: 00:04:22
RP: 12.0.9.2, RPF nbr: 12.0.9.2, RPF idx: eth-0-9
Upstream:
State: JOINED, SPT Switch: Enabled, JT Expiry: 40 secs
Macro state: Join Desired,
Downstream:
eth-0-3:
State: NO INFO, ET: off, PPT: off
Assert State: NO INFO, AT: off
Winner: 0.0.0.0, Metric: 4294967295, Pref: 4294967295, RPT bit: on
Macro state: Could Assert, Assert Track
Local Olist:
eth-0-3
```

### Related Commands

None

**8.4.30 show ip pim sparse-mode neighbor**

### Command Purpose

Use this command to show the neighbor information of pim sparse mode.

### Command Syntax

```
show ip pim sparse-mode neighbor ((IFNAME (address | )) | detail |
```
### Command Mode

Privileged EXEC

### Default

None

### Usage

None

### Examples

This example shows how to display the neighbor information of pim sparse mode:

```
Switch# show ip pim sparse-mode neighbor
```

<table>
<thead>
<tr>
<th>Neighbor Address</th>
<th>Interface</th>
<th>Uptime/Expires</th>
<th>Ver</th>
<th>DR Priority/Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0.9.2</td>
<td>eth-0-9</td>
<td>00:18:18</td>
<td>v2</td>
<td>DR</td>
</tr>
</tbody>
</table>

### Related Commands

None

#### 8.4.31 show ip pim sparse-mode rp mapping

### Command Purpose

Use this command to show group to rp mappings.

### Command Syntax

```
show ip pim sparse-mode rp mapping
```

### Command Mode

Privileged EXEC

### Default

None

### Usage

None

### Examples

This example shows how to display group to rp mappings:

```
Switch# show ip pim sparse-mode rp mapping
```

PIM group-to-RP mappings
Group(s): 224.0.0.0/4
RP: 12.0.9.2
  Info source: 12.0.9.2, via bootstrap, priority 192
  Uptime: 00:22:56, expires: 00:01:34

### Related Commands

None
8.4.32  show ip pim sparse-mode rp-hash

Command Purpose
Use this command to show the information of rp to be chosen based on group selected.

Command Syntax
show ip pim sparse-mode rp-hash GRP_ADDR

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRP_ADDR</td>
<td>Multicast group address</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to display the information of rp to be chosen based on group 224.0.0.10:

```bash
Switch# show ip pim sparse-mode rp-hash 224.0.0.10
RP: 12.0.9.2
Info source: 12.0.9.2, via bootstrap
```

Related Commands
None

8.4.33  show ip pim sparse-mode spt-threshold

Command Purpose
Use this command to show the rpt to spt threshold of pim sparse mode.

Command Syntax
show ip pim sparse-mode spt-threshold

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to display the rpt to spt threshold of pim sparse mode:

```bash
Switch# show ip pim sparse-mode spt-threshold
PIM spare-mode immediately switches over to SPT upon receiving the first traffic
```

Related Commands
None
8.4.34 show ip pim dense-mode interface

**Command Purpose**

Use this command to show the interface information of pim sparse mode.

**Command Syntax**

`show ip pim dense-mode interface { detail }`

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

This example shows how to display the interface information of pim dense mode:

```
Switch# show ip pim dense-mode interface
```

<table>
<thead>
<tr>
<th>Address</th>
<th>Interface</th>
<th>VIFIndex</th>
<th>Ver/Nbr</th>
<th>Mode</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.2.1</td>
<td>eth-0-2</td>
<td>0</td>
<td>v2/D</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3.3.3.1</td>
<td>eth-0-3</td>
<td>2</td>
<td>v2/D</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Related Commands**

None

8.4.35 show ip pim dense-mode mroute

**Command Purpose**

Use this command to show the mroute information of pim dense mode.

**Command Syntax**

`show ip pim dense-mode mroute`

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

This example shows how to display pim mroute information:

```
Switch# show ip pim dense-mode mroute
```

PIM-DM Multicast Routing Table
(2.2.2.2, 225.1.2.3)
- Source directly connected on eth-0-2
- State-Refresh Originator State: Originator
- Upstream IF: eth-0-2
- Upstream State: Forwarding
- Assert State: NoInfo
Downstream IF List:
  eth-0-3, in 'olist':
  Downstream State: Nolno
  Assert State: Nolno
(2.2.2.2, 225.1.2.4)
Source directly connected on eth-0-2
State-Refresh Originator State: Originator
Upstream IF: eth-0-2
  Upstream State: Forwarding
  Assert State: Nolno
Downstream IF List:
  eth-0-3, in 'olist':
  Downstream State: Nolno
  Assert State: Nolno

Related Commands
None

8.4.36 show ip pim dense-mode neighbor

Command Purpose
Use this command to show the neighbor information of pim dense mode.

Command Syntax
show ip pim sparse-mode neighbor { detail | }  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Detailed interface information</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to display the neighbor information of pim dense mode:
Switch# show ip pim dense-mode neighbor

<table>
<thead>
<tr>
<th>Neighbor-Address Interface</th>
<th>Uptime/Expires</th>
<th>Ver</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.4.4.4</td>
<td>eth-0-9</td>
<td>03d19h16m/00:01:29 v2</td>
</tr>
<tr>
<td>3.3.3.2</td>
<td>agg3</td>
<td>03d19h17m/00:01:37 v2</td>
</tr>
</tbody>
</table>

Related Commands
None

8.4.37 show ip pim dense-mode nexthop

Command Purpose
Use this command to show the nexthop information of pim dense mode.

Command Syntax
show ip pim sparse-mode nexthop
### Command Mode
Privileged EXEC

### Default
None

### Usage
None

### Examples
This example shows how to display the nexthop information of pim dense mode:
Switch# show ip pim dense-mode nexthop

<table>
<thead>
<tr>
<th>Destination</th>
<th>Nexthop Num</th>
<th>Nexthop Addr</th>
<th>Nexthop Interface</th>
<th>Metric Pref</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.2</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

### Related Commands
None

#### 8.4.38 show ip pim dense-mode interface

### Command Purpose
Use this command to show the interface information of pim sparse mode.

### Command Syntax
show ip pim dense-mode interface ( detail | )

### Command Mode
Privileged EXEC

### Default
None

### Usage
None

### Examples
This example shows how to display the interface information of pim dense mode:
Switch# show ip pim dense-mode interface

<table>
<thead>
<tr>
<th>Address</th>
<th>Interface</th>
<th>VIFIndex</th>
<th>Ver/ Nbr Mode</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.2.1</td>
<td>eth-0-2</td>
<td>0</td>
<td>v2/D</td>
<td>0</td>
</tr>
<tr>
<td>3.3.3.1</td>
<td>eth-0-3</td>
<td>2</td>
<td>v2/D</td>
<td>0</td>
</tr>
</tbody>
</table>

### Related Commands
None

#### 8.4.39 show ip pim dense-mode mroute

### Command Purpose
Use this command to show the mroute information of pim dense mode.

### Command Syntax
show ip pim dense-mode mroute
**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

This example shows how to display PIM mroute information:

Switch# show ip pim dense-mode mroute

PIM-DM Multicast Routing Table
(2.2.2.2, 225.1.2.3)
Source directly connected on eth-0-2
State-Refresh Originator State: Originator
Upstream IF: eth-0-2
Upstream State: Forwarding
Assert State: NoInfo

Downstream IF List:
eth-0-3, in 'olist':
Downstream State: NoInfo
Assert State: NoInfo

Related Commands
None

**8.4.40 show ip pim sparse-mode nexthop-virtual-pair**

**Command Purpose**

Use this command to show the PIM nexthop virtual address mapping information.

**Command Syntax**

show ip pim sparse-mode nexthop-virtual-pair

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

This example shows how to display the PIM nexthop virtual address mapping information:

Switch# show ip pim sparse-mode nexthop-virtual-pair

<table>
<thead>
<tr>
<th>pim nexthop address</th>
<th>virtual address</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.2</td>
<td>20.1.1.2</td>
</tr>
</tbody>
</table>

Related Commands
None
8.4.41 ip pim nexthop-address

Command Purpose
Use this command to set the virtual address of the pim nexthop address. To cancel this setting, use the no form of this command.

Command Syntax
ip pim nexthop-address NEXTHOP-ADDRESS virtual-address VIRTUAL-ADDRESS
no ip pim nexthop-address (NEXTHOP-ADDRESS | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEXTHOP-ADDRESS</td>
<td>nexthop address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>VIRTUAL-ADDRESS</td>
<td>virtual address</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
When PIM use virtual address to connect neighbour, Use this command to the virtual address of the pim nexthop address.

Examples
This example shows how to set a nexthop address with virtual address:
Switch# configure terminal
Switch(config-if)# ip pim nexthop-address 10.1.1.2 virtual-address 20.1.1.2
This example shows how to unset this setting:
Switch# configure terminal
Switch(config-if)# no ip pim nexthop-address

Related Commands
None

8.5 MVR Commands

8.5.1 Mvr

Command Purpose
Use this command to enable MVR. To disable MVR, use the no form of this command.

Command Syntax
mvr
no mvr

Command Mode
Global Configuration

Default
Disable

Usage
Enable MVR in the Switch, must disable ip multicast-routing before enable MVR.
Examples

This example shows how to enable MVR:

```
Switch# configure terminal
Switch(config)# no ip multicast-routing
Switch(config)# mvr
```

Related Commands

show mvr

8.5.2 mvr vlan

Command Purpose

Use this command to specify the MVR source vlan. To remove this setting, use the no form of this command.

Command Syntax

```
mvr vlan VLAN_ID
no mvr vlan
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

The related vlan interface should be created before the configuration of the MVR source vlan.

Examples

This example shows how to configure source vlan of MVR. configure vlan 2 as source vlan of MVR:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-if)# interface vlan 2
Switch(config-if)# mvr vlan 2
```

Related Commands

interface vlan

8.5.3 mvr group

Command Purpose

Use this command to configure global group for MVR. To remove this setting, use the no form of this command.

Command Syntax

```
mvr group IP_ADDR ( COUNT | )
no mvr group address ( COUNT | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>Multicast group address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>COUNT</td>
<td>Count of contiguous groups</td>
<td>1-64</td>
</tr>
</tbody>
</table>
### Command Mode

Global Configuration

### Default

None

### Usage

This command is used to create or delete a global static group.

### Examples

This example shows how to create global static group from 238.255.0.1 to 238.255.0.50:

```
Switch# configure terminal
Switch(config)# mvr group 238.255.0.1 50
```

### Related Commands

None

#### 8.5.4 mvr source-address

### Command Purpose

Use this command to create or delete mvr source address. To remove this setting, use the no form of this command.

### Command Syntax

```
mvr source-address IP_ADDR
no mvr source-address
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>Source ip address</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

### Command Mode

Global Configuration

### Default

10.0.0.1

### Usage

None

### Examples

Create mvr source address:

```
Switch# configure terminal
Switch(config)# mvr source-address 192.168.11.1
```

Resume mvr source address as default IP address:

```
Switch# configure terminal
Switch(config)# no mvr source-address
```

### Related Commands

None

#### 8.5.5 mvr type

### Command Purpose

Use this command to configure a switch-port as source port or receiver port. To remove this setting, use the no form of this command.
Command Syntax

mvr type (source | receiver vlan VLAN_ID)
no mvr type (receiver vlan VLAN_ID |

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>MVR source port</td>
<td>-</td>
</tr>
<tr>
<td>receiver</td>
<td>MVR receiver port</td>
<td>-</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>MVR receiver vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
None

Usage
Before configure the interface as source port or receiver port, make sure the source port belong to source vlan, and the receiver port must not belong to source vlan.

Examples
Configure the eth-0-1 as source port, and configure the eth-0-2 as receiver port of vlan 2:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# mvr type source
Switch(config)# interface eth-0-2
Switch(config-if)# mvr type receiver vlan 2

Related Commands
None

8.5.6 show mvr

Command Purpose
Use this command to show mvr information.

Command Syntax
show mvr

Command Mode
Privileged EXEC

Default
None

Usage
Show mvr information.

Examples
This example shows how to display MVR information:
Switch# show mvr

MVR Running: TRUE
MVR Multicast VLAN: 10
MVR Source-address: 1.1.1.1
MVR Max Multicast Groups: 512
8.5.7 show mvr interface

**Command Purpose**
Use this command to show mvr interface information.

**Command Syntax**
show mvr interface

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
Show mvr interface information.

**Examples**
This example shows how to display MVR interface information:

```
Switch# show mvr interface
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>VLAN</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-0-2</td>
<td>source</td>
<td>10</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>eth-0-1</td>
<td>receiver</td>
<td>11</td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>

**Related Commands**
None

8.5.8 show mvr group

**Command Purpose**
Use this command to show mvr group learned from receiver port.

**Command Syntax**
show mvr group vlan VLAN_ID (GRP_ADDR | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>MVR receiver vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>GRP_ADDR</td>
<td>Multicast group address</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
Show mvr group information learned from receiver port
Examples

This example shows how to display mvr group learned from receiver port:
Switch# show mvr groups

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Interface</th>
<th>Group-Address</th>
<th>Uptime</th>
<th>Expires-time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>eth-0-1</td>
<td>227.0.0.1</td>
<td>00:25:51</td>
<td>00:04:19</td>
</tr>
</tbody>
</table>

Related Commands

None

8.5.9 show mvr group static

Command Purpose

Use this command to show mvr global static groups.

Command Syntax

show mvr group static global

Command Mode

Privileged EXEC

Default

None

Usage

Show mvr static configured group information.

Examples

This example shows how to display mvr global static groups:
Switch# show mvr groups static global

MVR Static Global Group:
227.0.0.1
227.0.0.2
227.0.0.3
227.0.0.4
227.0.0.5
227.0.0.6
227.0.0.7
227.0.0.8
227.0.0.9
227.0.0.10

Related Commands

None

8.5.10 show resource mvr

Command Purpose

Use this command to display the resource usage of MVR.

Command Syntax

show resource mvr

Command Mode

Privileged EXEC
Default
None

Usage
None

Examples
This example shows how to display the resource usage of MVR:

Switch# show resource mvr

<table>
<thead>
<tr>
<th>MVR Resource</th>
<th>Used</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>MVR Entry</td>
<td>0</td>
<td>511</td>
</tr>
<tr>
<td>MVR Member</td>
<td>0</td>
<td>1022</td>
</tr>
</tbody>
</table>

Related Commands
None
Chapter 9 IPv6 Multicast Commands

9.1 IPv6 Multicast-Routing Commands

9.1.1 Ipv6 multicast-routing

Command Purpose

Use this command to enable ipv6 multicast routing.
To disable ipv6 multicast routing, use the no form of this command.

Command Syntax

ipv6 multicast-routing
no ipv6 multicast-routing

Command Mode

Global Configuration

Default
Enable

Usage
None

Examples

This example shows how to enable ipv6 multicast routing:

Switch# configure terminal
Switch(config)# ipv6 multicast-routing

This example shows how to disable ipv6 multicast routing:

Switch# configure terminal
Switch(config)# no ipv6 multicast-routing

Related Commands

None
9.1.2 ipv6 multicast route-limit

Command Purpose

Use this command to set the maximum number of the multicast routes.
To reset it to default value, use the no form of this command.

Command Syntax

ipv6 multicast route-limit LIMIT (THRESHOLD |)
no ipv6 multicast route-limit

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIMIT</td>
<td>Max number of multicast route entries</td>
<td>1-2048</td>
</tr>
<tr>
<td>THRESHOLD</td>
<td>Threshold at which to generate warning message</td>
<td>1-2048</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

Default maximum number of the multicast routes should be 2048.
Default threshold should be same as the maximum number of multicast routes.

Usage

None

Examples

This example shows how to set the maximum number of the multicast routes to 512:
Switch# configure terminal
Switch(config)# ipv6 multicast route-limit 512

This example shows how to reset the maximum number of the multicast routes to default value:
Switch# configure terminal
Switch(config)# no ipv6 multicast route-limit

Related Commands

show ipv6 mroute route-limit
9.1.3 show ipv6 mroute

Command Purpose

Use this command to display the ipv6 multicast routing table information.

Command Syntax

show ipv6 mroute ( sparse | ) ( count | summary | )
show ipv6 mroute IPV6_ADDR ( sparse | ) ( count | summary | )
show ipv6 mroute route-limit

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>sparse</td>
<td>Show sparse multicast routes</td>
<td>-</td>
</tr>
<tr>
<td>count</td>
<td>Show number of multicast route entries</td>
<td>-</td>
</tr>
<tr>
<td>summary</td>
<td>Show abbreviated multicast route information</td>
<td>-</td>
</tr>
<tr>
<td>IPV6_ADDR</td>
<td>Show specify source or group address multicast route</td>
<td>IPv6 address</td>
</tr>
<tr>
<td>route-limit</td>
<td>Show max route limit value</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display multicast routing table:

Switch# show ipv6 mroute
IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface
2001:1:1234, ff0e::1234:5678
time: 00:00:02, stat expires 00:03:28
Owner PIM-SMv6, Flags: TF
This example shows how to display multicast routing table summary information:

Switch# show ipv6 mroute summary

IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface
2001:1::1234, ff0e::1234:5678
  00:01:04/00:02:26, PIM-SMv6, Flags: TF

Related Commands

ipv6 multicast route-limit
ipv6 mroute-rpf

9.1.4 show ipv6 mif

Command Purpose

Use this command to display the multicast interface information.

Command Syntax

show ipv6 mif { IFNAME | }

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None
Examples

This example shows how to display multicast interface information:

Switch# show ipv6 mif

<table>
<thead>
<tr>
<th>Interface</th>
<th>Mif</th>
<th>Owner</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth-0-1</td>
<td>0</td>
<td>PIM-SMv6</td>
<td>00:00:05</td>
</tr>
<tr>
<td>Register</td>
<td>1</td>
<td>PIM-SMv6</td>
<td>00:00:05</td>
</tr>
</tbody>
</table>

Related Commands

ipv6 pim sparse-mode

9.1.5 show ipv6 multicast groups count

Command Purpose

Use this command to display the multicast group count.

Command Syntax

show ipv6 multicast groups count

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display multicast group number:

Switch# show ipv6 multicast groups count

multicast group record count:  1
multicast source record count: 0
multicast total record count:  1
multicast max record count: 2048

Related Commands
None

9.1.6 show resource mcast6

Command Purpose
Use this command to display ipv6 multicast resource information.

Command Syntax
show resource mcast6

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to display ipv6 multicast resource information:
Switch# show resource mcast6

<table>
<thead>
<tr>
<th>MCAST</th>
<th>Resource</th>
<th>Used</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mcast Entry</td>
<td>0</td>
<td>224</td>
</tr>
<tr>
<td></td>
<td>Mcast Member</td>
<td>0</td>
<td>1792</td>
</tr>
</tbody>
</table>

Related Commands
None
9.1.7 clear ipv6 mroute

Command Purpose

Use this command to clear the ipv6 multicast routing table information.

Command Syntax

clear ipv6 mroute (* | GRP_IPV6_ADDR | SRC_IPV6_ADDR | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRP_IPV6_ADDR</td>
<td>Clear specify group address multicast route</td>
<td>IPv6 address</td>
</tr>
<tr>
<td>SRC_IPV6_ADDR</td>
<td>Clear specify source address multicast route</td>
<td>IPv6 address</td>
</tr>
<tr>
<td>*</td>
<td>Clear all multicast routes</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to clear all ipv6 multicast routing table information:

Switch# clear ipv6 mroute *

Related Commands

show ipv6 mroute

9.2 MLD Commands

9.2.1 ipv6 mld access-group

Command Purpose

Use this command to apply an access-list to the mld interface.

To remove this setting, use the no form of this command.
**Command Syntax**

```
ipv6 mld access-group LISTNAME
no ipv6 mld access-group
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISTNAME</td>
<td>The name of the ipv6 access-list to be applied.</td>
<td>A string with 1-20 characters</td>
</tr>
<tr>
<td></td>
<td>The format of access-list should be ipv6.</td>
<td></td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

Access-group is not configured on any mld interface by default.

**Usage**

No matter the source ipv6 prefix or the destination ipv6 prefix in ACE should take effect respectively. If ACE’s action is deny, then the packet will be ignored; Otherwise if it matches one whose action is permit, then it will be processed regularly.

**Examples**

This example shows how to apply the access-list acl1 to the interface vlan1:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 mld access-group acl1
```

This example shows how to remove the access-list acl1 on the interface:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ipv6 mld access-group
```

**Related Commands**

```
show ipv6 mld interface
```

**9.2.2 ipv6 mld immediate-leave group-list**

**Command Purpose**

Use this command to apply an access-list to configure which groups support immediately-leave per interface. To remove this setting, use the no form of this command.
## Command Syntax

```
ipv6 mld immediate-leave group-list LISTNAME
no ipv6 mld immediate-leave
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISTNAME</td>
<td>The name of the ipv6 access-list to be applied. The format of access-list should be ipv6.</td>
<td>-</td>
</tr>
</tbody>
</table>

## Command Mode

Interface Configuration

## Default

Access-group is not configured on any mld interface by default.

## Usage

No matter the source ipv6 prefix or the destination ipv6 prefix in ACE should be take effect respectively. If ACE’s action is denied, then the packet should be ignored; Otherwise if it matches one whose action is permit, then it should be processed regularly.

## Examples

This example shows how to apply an access-list to configure which groups support immediately-leave on interface vlan1:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 mld immediate-leave group-list acl1
```

This example shows how to remove the access-list acl1 on the interface:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ipv6 mld immediate-leave group-list
```

## Related Commands

show ipv6 mld interface

## 9.2.3 ipv6 mld last-member-query-count

## Command Purpose

Use this command to set the value of last member query count. To return it to default value, use the no form of this command.
**Command Syntax**

```
ipv6 mld last-member-query-count COUNT
no ipv6 mld last-member-query-count
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>COUNT</td>
<td>The value of last member query count, range is 2 to 7</td>
<td>2-7</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

2

**Usage**

None

**Examples**

This example shows how to set the value of last member query count to 5:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 mld last-member-query-count 5
```

This example shows how to return the value of last member query count to default value:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ipv6 mld last-member-query-count
```

**Related Commands**

- show ipv6 mld interface
- ipv6 mld last-member-query-interval

**9.2.4 ipv6 mld last-member-query-interval**

**Command Purpose**

Use this command to set the value of last member query interval.
To reset it to default value, use the no form of this command.
**Command Syntax**

```
ipv6 mld last-member-query-interval INTERVAL
no ipv6 mld last-member-query-interval
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>The last member query interval value(ms)</td>
<td>1000-25500</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

1000

**Usage**

None

**Examples**

This example shows how to set the last member query interval value to 10000ms:

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping last-member-query-interval 2000
```

This example shows how to reset the last member query interval value to default value:

```
Switch# configure terminal
Switch(config)# no ipv6 mld snooping last-member-query-interval
```

**Related Commands**

show ipv6 mld interface
ipv6 mld last-member-query-count

**9.2.5 ipv6 mld limit**

**Command Purpose**

Use this command to set the max num of groups allowed.
To reset it to default value, use the no form of this command.

**Command Syntax**

```
ipv6 mld limit NUMBER ( except LISTNAME )
```
no ipv6 mld limit

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>The max num of groups, range is 1 to 4096</td>
<td>1-4096</td>
</tr>
<tr>
<td>LISTNAME</td>
<td>Groups not to be counted</td>
<td>A string with 1-20 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration & Interface Configuration

**Default**

4096

**Usage**

Max number of groups is 4096 by default, in global configuration mode, use this command to set number of groups for all ports, in interface configuration mode, use this command to set number of groups for one port.

**Examples**

This example shows how to set the max num of groups allowed to 1000 globally:

```
Switch# configure terminal
Switch(config)# ipv6 mld limit 1000
```

This example shows how to reset the max num of groups to default value:

```
Switch# configure terminal
Switch(config)# no ipv6 mld limit
```

**Related Commands**

show ipv6 mld interface

**9.2.6 ipv6 mld mroute-proxy**

**Command Purpose**

Use this command to set the mroute-proxy port on this interface. To remove it, use the no form of this command.

**Command Syntax**

ipv6 mld mroute-proxy IFNAME

no ipv6 mld mroute-proxy IFNAME
**Parameter** | **Parameter Description** | **Parameter Value**
--- | --- | ---
IFNAME | The interface name of the mroute-proxy port | Support physical/aggregation/loopback/vlan/tunnel ports

**Command Mode**

**Interface Configuration**

**Default**

None

**Usage**

This command is used to set the mroute-proxy port on the interface. Only one mroute-proxy port can be set on the interface. When set it again, the new setting will overwrite the old one.

**Examples**

This example shows how to set the mroute-proxy port to eth-0-1 on this interface:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 mld mroute-proxy eth-0-1
```

This example shows how to remove the mroute-proxy port on this interface:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ipv6 mld mroute-proxy
```

**Related Commands**

ipv6 mld proxy-service

**9.2.7 ipv6 mld proxy-service**

**Command Purpose**

Use this command to enable mld mroute proxy service on the interface.

To disable it, use the no form of this command.

**Command Syntax**

ipv6 mld proxy-service

no ipv6 mld proxy-service
**Command Mode**

Interface Configuration

**Default**

None

**Usage**

This command is used with command ipv6 mld mroute-proxy and to set the upstream interface of the mld group.

**Examples**

This example shows how to enable mld mroute proxy service on this interface:

Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 mld proxy-service

This example shows how to disable mld mroute proxy service:

Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ipv6 mld proxy-service

**Related Commands**

ipv6 mld mroute-proxy

**9.2.8 ipv6 mld querier-timeout**

**Command Purpose**

Use this command to set the mld previous querier timeout value.
To reset it to default value, use the no form of this command.

**Command Syntax**

ipv6 mld querier-timeout INTERVAL
no ipv6 mld querier-timeout

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>The mld previous querier timeout value, range is 60 to 300s.</td>
<td>60-300</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration
**Default**

255s

**Usage**

None

**Examples**

This example shows how to set the mld previous querier timeout value to 100 seconds:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 mld querier-timeout 100
```

This example shows how to reset the mld previous querier timeout value to default value:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ipv6 mld querier-timeout
```

**Related Commands**

ipv6 mld query-interval
ipv6 mld query-max-response-time

**9.2.9 ipv6 mld query-interval**

**Command Purpose**

Use this command to set the mld query interval.
To reset it to default value, use the no form of this command.

**Command Syntax**

```
ipv6 mld query-interval INTERVAL
no ipv6 mld query-interval
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>The value of mld query interval, range is 2 to 18000s.</td>
<td>2-18000</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

125s
Usage

None

Examples

This example shows how to set the mld query interval to 300 seconds:

Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 mld query-interval 300

This example shows how to return the mld query interval to default value:

Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ipv6 mld query-interval

Related Commands

ipv6 mld querier-timeout
ipv6 mld query-max-response-time

9.2.10  ipv6 mld query-max-response-time

Command Purpose

Use this command to set the mld query max response time.
To reset it to default value, use the no form of this command.

Command Syntax

ipv6 mld query-max-response-time INTERVAL
no ipv6 query-max-response-time

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>The mld query max response time, range is 1 to 25s.</td>
<td>1-25</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

10s

Usage

Query max response time must be less than mld query interval.
Examples
This example shows how to set the mld query max response time to 20 seconds:

Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 mld query-max-response-time 20

This example shows how to return the mld query max response time to default value:

Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ipv6 mld query-max-response-time

Related Commands
ipv6 mld querier-timeout
ipv6 mld query-interval

9.2.11 ipv6 mld robustness-variable

Command Purpose
Use this command to set the mld querier robustness variable value.
To reset it to default value, use the no form of this command.

Command Syntax
ipv6 mld robustness-variable VALUE
no ipv6 mld robustness-variable

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VALUE</td>
<td>The mld querier robustness variable value, range is 2 to 7.</td>
<td>2-7</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
2

Usage
None

Examples
This example shows how to set the mld querier robustness variable value to 6:

Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 mld robustness-variable 6
This example shows how to reset the mld querier robustness variable value to default value:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ipv6 mld robustness-variable
```

**Related Commands**

show ipv6 mld interface

### 9.2.12 ipv6 mld version

**Command Purpose**

Use this command to set the mld version on interface.
To return it to default value, use the no form of this command.

**Command Syntax**

```
ipv6 mld version NUMBER
no ipv6 version
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>The mld version on the interface</td>
<td>1-2</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

1

**Usage**

None

**Examples**

This example shows how to set the mld version 2 on the interface:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 mld version 2
```

This example shows how to return the mld version to default value:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ipv6 mld version
```

**Related Commands**

show ipv6 mld interface
9.2.13 ipv6 mld static-group

Command Purpose

Use this command to configure the static multicast group on interface.
To delete static group, use the no form of this command.

Command Syntax

ipv6 mld static-group GRP_IPV6_ADDR ( source SRC_IPV6_ADDR | )
no ipv6 mld static-group GRP_IPV6_ADDR ( source SRC_IPV6_ADDR | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRP_IPV6_ADDR</td>
<td>The multicast group address</td>
<td>IPv6 address</td>
</tr>
<tr>
<td>SRC_IPV6_ADDR</td>
<td>The multicast source address</td>
<td>IPv6 address</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

This example shows how to configure the static mld group on interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 mld static-group ff0e::1234
Switch(config-if)# ipv6 mld static-group ff0e::1234 source 2001::2
```

This example shows how to delete static mld group on interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ipv6 mld static-group ff02::1234
```

Related Commands

show ipv6 mld groups
9.2.14 ipv6 mld ssm-map enable

**Command Purpose**

Use this command to enable mld ssm mapping.  
To disable ssm mapping, use the no form of this command.

**Command Syntax**

ipv6 mld ssm-map enable  
no ipv6 mld ssm-map enable

**Command Mode**

Global Configuration

**Default**

Disable

**Usage**

None

**Examples**

This example shows how to enable mld ssm mapping:

```
Switch# configure terminal
Switch(config)# ipv6 mld ssm-map enable
```

This example shows how to disable mld ssm mapping:

```
Switch# configure terminal
Switch(config)# no ipv6 mld ssm-map enable
```

**Related Commands**

None

9.2.15 ipv6 mld ssm-map static

**Command Purpose**

Use this command to set mld ssm mapping.  
To cancel ssm mapping setting, use the no form of this command.
Command Syntax

ipv6 mld ssm-map static LISTNAME SRC_IPV6_ADDR
no ipv6 mld ssm-map static LISTNAME SRC_IPV6_ADDR

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISTNAME</td>
<td>Specify multicast group address range</td>
<td>A string with 1-20 characters</td>
</tr>
<tr>
<td></td>
<td>access list</td>
<td></td>
</tr>
<tr>
<td>SRC_IPV6_ADDR</td>
<td>Multicast source address</td>
<td>IPv6 address</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

Disable

Usage

None

Examples

This example shows how to set mld ssm mapping:

Switch# configure terminal
Switch(config)# ipv6 mld ssm-map static ipacl 2001::2

This example shows how to unset mld ssm mapping:

Switch# configure terminal
Switch(config)# no ipv6 mld ssm-map static ipacl 2001::2

Related Commands

None

9.2.16 clear ipv6 mld

Command Purpose

Use this command to clear mld groups.

Command Syntax

clear ipv6 mld group (*|IPV6_ADDR)
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>All multicast group address</td>
<td>-</td>
</tr>
<tr>
<td>IPV6_ADDR</td>
<td>Specify multicast group address</td>
<td>IPv6 address</td>
</tr>
</tbody>
</table>

### Command Mode

Privileged EXEC

### Default

None

### Usage

None

### Examples

This example shows how to clear mld group all:

```
Switch# clear ipv6 mld
Switch# clear ipv6 mld group *
```

This example shows how to clear mld specified group:

```
Switch# clear ipv6 mld group ff02::1234
```

### Related Commands

- `show ipv6 mld groups`

### 9.2.17 clear ipv6 mld interface

#### Command Purpose

Use this command to clear mld groups on specified interface.

#### Command Syntax

```
clear ipv6 mld ( group IPV6_ADDR | interface ) IFNAME
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPV6_ADDR</td>
<td>Specify multicast group address</td>
<td>IPv6 address</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>
Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to clear mld group on specified interface:

Switch# clear ipv6 mld group interface eth-0-1

Related Commands

show ipv6 mld groups

9.2.18 show ipv6 mld groups

Command Purpose

Use this command to show the information about mld groups.

Command Syntax

show ipv6 mld groups IPV6_ADDR ( detail | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPV6_ADDR</td>
<td>Specify multicast group address</td>
<td>IPv6 address</td>
</tr>
<tr>
<td>detail</td>
<td>Detailed Information</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None
Usage

None

Examples

This example shows how to display the detail information about mld groups:

Switch# show ipv6 mld groups detail

MLD Connected Group Membership Details for eth-0-2
 Interface:  eth-0-2
 Group:  ff0e::1234:5678
 Uptime:  00:00:10
 Group mode:  Exclude (Expires: 00:04:10)
 Source list is empty

Related Commands

None

9.2.19  show ipv6 mld groups interface

Command Purpose

Use this command to show the information about mld groups on interface.

Command Syntax

show ipv6 mld groups IFNAME ( IPV6_ADDR | ( detail | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
<tr>
<td>IPV6_ADDR</td>
<td>Specify multicast group address</td>
<td>IPv6 address</td>
</tr>
<tr>
<td>detail</td>
<td>Detailed Information</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None
Usage

None

Examples

This example shows how to display the information about mld groups on interface eth-0-1:

```
Switch# show ipv6 mld groups eth-0-1
MLD Connected Group Membership
Group Address          Interface    Expires
ff0e::1234:5678          eth-0-2     00:03:01
```

Related Commands

None

9.2.20 show ipv6 mld groups count

Command Purpose

Use this command to show mld group number.

Command Syntax

```
show ipv6 mld groups (IFNAME | ) count
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None
Examples

This example shows how to display the mld group number on interface eth-0-1:

Switch# show ipv6 mld groups eth-0-1 count

Dynamic multicast groups count: 1
Static multicast groups count: 0
Total multicast groups count: 1

Related Commands

None

9.2.21  show ipv6 mld interface

Command Purpose

Use this command to show the information about mld on interface.

Command Syntax

show ipv6 mld interface ( IFNAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the information about mld on interface eth-0-1:

Switch# show ipv6 mld interface eth-0-1
Interface eth-0-1 (Index 1)
MLD Active, Querier, Version 1 (default)
Internet address is fe80::9c7c:7eff:fe94:8300
MLD interface has 0 group-record states
MLD activity: 0 joins, 0 leaves
MLD query interval is 125 seconds
MLD querier timeout is 255 seconds
MLD max query response time is 10 seconds
Last member query response interval is 1000 milliseconds
Group Membership interval is 260 seconds

Related Commands

None

9.3 MLD Snooping Commands

9.3.1 ipv6 mld snooping

Command Purpose

Use this command to enable mld snooping.
To disable mld snooping, use the no form of this command.

Command Syntax

ipv6 mld snooping ( vlan VLAN_ID )
no ipv6 mld snooping ( vlan VLAN_ID )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

Disable

Usage

Mld Snooping can be enabled globally and per vlan. By default, mld snooping should be disabled globally and per vlan.
Examples

This example shows how to enable mld snooping:
Switch# configure terminal
Switch(config)# ipv6 mld snooping

This example shows how to disable mld snooping:
Switch# configure terminal
Switch(config)# no ipv6 mld snooping

This example shows how to enable mld snooping on vlan 10:
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 10

This example shows how to disable mld snooping on vlan 10:
Switch# configure terminal
Switch(config)# no ipv6 mld snooping vlan 10

Related Commands

show ipv6 mld snooping

9.3.2 ipv6 mld snooping fast-leave

Command Purpose

Use this command to enable mld snooping fast leave.
To disable it, use the no form of this command.

Command Syntax

ipv6 mld snooping ( vlan VLAN_ID | ) fast-leave
no ipv6 mld snooping ( vlan VLAN_ID | ) fast-leave

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

Disable

Usage

This command will override immediate-leave setting.
Examples

This example shows how to enable mld snooping fast-leave:
Switch# configure terminal
Switch(config)# ipv6 mld snooping fast-leave

This example shows how to disable mld snooping fast-leave:
Switch# configure terminal
Switch(config)# no ipv6 mld snooping fast-leave

Related Commands

show ipv6 mld snooping global

9.3.3 ipv6 mld snooping last-member-query-interval

Command Purpose

Use this command to set the last member query interval of mld snooping. To reset it to default value, use the no form of this command.

Command Syntax

ipv6 mld snooping ( vlan VLAN_ID | ) last-member-query-interval INTERVAL
no ipv6 mld snooping ( vlan VLAN_ID | ) last-member-query-interval

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>INTERVAL</td>
<td>The last member query interval</td>
<td>1000-25500</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

1000ms

Usage

Mld last member query interval can be configured per vlan. The default is 1000ms and the range is 1000-25500ms.

Examples

This example shows how to set the last member query interval:
Switch# configure terminal
Switch(config)# ipv6 mld snooping last-member-query-interval 2000
This example shows how to reset the last member query interval to default value:

Switch# configure terminal
Switch(config)# no ipv6 mld snooping last-member-query-interval

Related Commands

show ipv6 mld snooping
show ipv6 mld snooping vlan

9.3.4 ipv6 mld snooping global source-address

Command Purpose

Use this command to set the global source address.
To reset it to default value, use the no form of this command.

Command Syntax

ipv6 mld snooping global source-address IPV6_ADDR
no ipv6 mld snooping global source-address

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPV6_ADDR</td>
<td>The IPv6 address of source address</td>
<td>IPv6 Address</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

The default IPv6 address is :: (All zero in 128 bits IPv6 address)

Usage

Will use global configured source-address if vlan is not configured. otherwise, use source-address config from vlan.

Examples

This example shows how to set the global source address to fe80::1:

Switch# configure terminal
Switch(config)# ipv6 mld snooping global-source-address fe80::1

This example shows how to reset the global source address to default value:

Switch# configure terminal
Switch(config)# no ipv6 mld snooping global-source-address
Related Commands

show ipv6 mld snooping querier

9.3.5  ipv6 mld snooping max-member-num

Command Purpose

Use this command to set the max allowed member number. To reset it to default value, use the no form of this command.

Command Syntax

ipv6 mld snooping ( vlan VLAN_ID | ) max-member-num NUMBER
no ipv6 mld snooping ( vlan VLAN_ID | ) max-member-num

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>NUMBER</td>
<td>The max member number of mld snooping</td>
<td>1-4096</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

4096

Usage

None

Examples

This example shows how to set the max member number of mld snooping to 1024:

Switch# configure terminal
Switch(config)# ipv6 mld snooping max-member-num 1024

This example shows how to reset the max member number to default value:

Switch# configure terminal
Switch(config)# no ipv6 mld snooping max-member-num

Related Commands

show ipv6 mld snooping global
show ipv6 mld snooping vlan
9.3.6 ipv6 mld snooping query-interval

Command Purpose

Use this command to set the mld snooping query-interval. To reset the query-interval to default value, use the no form of this command.

Command Syntax

ipv6 mld snooping ( vlan VLAN_ID | ) query-interval INTERVAL
no ipv6 mld snooping ( vlan VLAN_ID | ) query-interval

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>INTERVAL</td>
<td>The query-interval of mld snooping (seconds), range is 2 to 18000</td>
<td>2-18000</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

125s

Usage

Query interval can’t less than the mld snooping query max response time.

Examples

This example shows how to set the mld snooping query interval to 64s:

Switch# configure terminal
Switch(config)# ipv6 mld snooping query-interval 64

This example shows how to reset the query-interval to default value:

Switch# configure terminal
Switch(config)# no ipv6 mld snooping query-interval

Related Commands

show ipv6 mld snooping querier
show ipv6 mld snooping querier vlan
9.3.7 ipv6 mld snooping query-max-response-time

Command Purpose

Use this command to set the mld snooping query-interval. To return the query-interval to default value, use the no form of this command.

Command Syntax

ipv6 mld snooping ( vlan VLAN_ID | ) query-max-response-time TIME
no ipv6 mld snooping ( vlan VLAN_ID | ) query-max-response-time

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>TIME</td>
<td>The query max response time (seconds)</td>
<td>1-25</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

10s

Usage

Query interval can’t less than the mld snooping query max response time.

Examples

This example shows how to set the mld snooping query max response time to 15s:

Switch# configure terminal
Switch(config)# ipv6 mld snooping query-max-response-time 15

This example shows how to return the query max response time to default value:

Switch# configure terminal
Switch(config)# no ipv6 mld snooping query-max-response-time

Related Commands

show ipv6 mld snooping querier
show ipv6 mld snooping querier vlan
9.3.8 ipv6 mld snooping report-suppression

**Command Purpose**

Use this command to enable report suppression.
To disable report suppression, use the no form of this command.

**Command Syntax**

ipv6 mld snooping (vlan VLAN_ID | ) report-suppression
no ipv6 mld snooping (vlan VLAN_ID | ) report-suppression

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

Enable

**Usage**

Will not do report suppression when MLD snooping works in v2 mode.

**Examples**

This example shows how to enable the report suppression:
Switch# configure terminal
Switch(config)# ipv6 mld snooping report-suppression

This example shows how to disable report suppression:
Switch# configure terminal
Switch(config)# no ipv6 mld snooping report-suppression

**Related Commands**

show ipv6 mld snooping
show ipv6 mld snooping vlan
9.3.9 ipv6 mld snooping version

Command Purpose

Use this command to set the mld snooping version.
To return it to default value, use the no form of this command.

Command Syntax

ipv6 mld snooping (vlan VLAN_ID | ) version VERSION
no ipv6 mld snooping (vlan VLAN_ID | ) version

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>VERSION</td>
<td>Mld snooping version, range is 1 to 2.</td>
<td>1-2</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

1

Usage

The default version is 1.

Examples

This example shows how to set the mld snooping version 2:

Switch# configure terminal
Switch(config)# ipv6 mld snooping version 2

Related Commands

show ipv6 mld snooping
show ipv6 mld snooping vlan

9.3.10 ipv6 mld snooping discard-unknown

Command Purpose

Use this command to enable discard unknown.
To disable discard unknown, use the no form of this command.

Command Syntax

ipv6 mld snooping (vlan VLAN_ID | ) discard-unknown
no ipv6 mld snooping (vlan VLAN_ID | ) discard-unknown
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
Enabled by default, unknown multicast traffic will flood in vlan.

**Usage**
None

**Examples**
This example shows how to enable discard-unknown multicast traffic:
```
Switch# configure terminal
Switch(config)# ipv6 mld snooping discard-unknown
```

**Related Commands**
show ipv6 mld snooping
show ipv6 mld snooping vlan

### 9.3.11 ipv6 mld snooping querier tcn

**Command Purpose**
Use this command to set MLD snooping querier TCN related parameters. To reset it to default value, use the no form of this command.

**Command Syntax**
```
ipv6 mld snooping querier tcn ( enable | query-count COUNT | query-interval INTERVAL | query-max-response-time TIME )
no ipv6 mld snooping querier tcn ( enable | query-count | query-interval | query-max-response-time )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>MLD querier TCN query enable</td>
<td>-</td>
</tr>
<tr>
<td>COUNT</td>
<td>MLD querier TCN query count, default is 2.</td>
<td>1-10</td>
</tr>
<tr>
<td>INTERVAL</td>
<td>MLD querier TCN query interval, default is 10s.</td>
<td>1-255 seconds</td>
</tr>
<tr>
<td>TIME</td>
<td>MLD querier TCN query max response time, default is 5s</td>
<td>1-9 seconds</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
This feature is enabled by default, default query count is 2, default query interval is 10s, maximum response time is 5s

**Usage**
None
Examples

This example shows how to use ipv6 mld snooping querier tcn command:

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping querier tcn query-count 2
```

Related Commands

show ipv6 mld snooping querier

9.3.12 ipv6 mld snooping vlan access-group

Command Purpose

Use this command to set mld snooping access group on vlan.

Command Syntax

ipv6 mld snooping vlan vlan_id access-group acl
no ipv6 mld snooping vlan vlan_id access-group

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan_id</td>
<td>Vlan ID, range is 1 to 4094.</td>
<td>1-4094</td>
</tr>
<tr>
<td>acl</td>
<td>IPV6 Named Standard Access list.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This example shows how to use apply access-group on vlan 10:

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 10 access-group acl
```

This example shows how to remove access-group from vlan 10:

```
Switch# configure terminal
Switch(config)# no ipv6 mld snooping vlan 10 access-group
```
Related Commands

show ipv6 mld snooping vlan

9.3.13  ipv6 mld snooping vlan mrouter interface

Command Purpose

Use this command to set mld snooping mrouter interface on vlan.

Command Syntax

ipv6 mld snooping vlan VLAN_ID mrouter interface IFNAME
no ipv6 mld snooping vlan vlan_id mrouter interface IFNAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Mrouter interface on this vlan</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

The specified interface must have already joined the configured vlan.

Examples

This example shows how to set eth-0-1 as mrouter interface on vlan 10:

Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 10 mrouter interface eth-0-1

This example shows how to unset eth-0-1 as mrouter interface on vlan 10:

Switch# configure terminal
Switch(config)# no ipv6 mld snooping vlan 10 mrouter interface eth-0-1

Related Commands

show ipv6 mld snooping vlan
9.3.14 ipv6 mld snooping vlan mrouter-aging-interval

**Command Purpose**

Use this command to set mld snooping mrouter interface aging interval on vlan.

**Command Syntax**

ipv6 mld snooping vlan VLAN_ID mrouter-aging-interval INTERVAL
no ipv6 mld snooping vlan VLAN_ID mrouter-aging-INTERVAL

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>INTERVAL</td>
<td>Dynamic mrouter interface aging interval on this vlan(seconds)</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

255s

**Usage**

None

**Examples**

This example shows how to set dynamic mrouter interface aging interval as 100 seconds on vlan 10:

Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 10 mrouter-aging-interval 100

This example shows how to reset dynamic mrouter interface aging interval as default on vlan 10:

Switch# configure terminal
Switch(config)# no ipv6 mld snooping vlan 10 mrouter-aging-interval

**Related Commands**

show ipv6 mld snooping vlan
9.3.15 ipv6 mld snooping vlan querier

Command Purpose

Use this command to enable mld snooping querier on vlan.

Command Syntax

ipv6 mld snooping vlan VLAN_ID querier
no ipv6 mld snooping vlan VLAN_ID querier

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

Disable

Usage

None

Examples

This example shows how to enable querier on vlan 10:
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 10 querier

This example shows how to disable querier on vlan 10:
Switch# configure terminal
Switch(config)# no ipv6 mld snooping vlan 10 querier

Related Commands

show ipv6 mld snooping querier vlan

9.3.16 ipv6 mld snooping vlan querier address

Command Purpose

Use this command to set mld snooping querier address on vlan.
Command Syntax

ipv6 mld snooping vlan VLAN_ID querier address IPV6_ADDR
no ipv6 mld snooping vlan VLAN_ID querier address IPV6_ADDR

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>IPV6_ADDR</td>
<td>The address of querier on this vlan</td>
<td>IPv6 Address</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

Will use global configured source-address if vlan is not configured. otherwise, use source-address config from vlan.

Examples

This example shows how to set querier address on vlan 10:

Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 10 querier address fe80::1

This example shows how to unset querier address on vlan 10:

Switch# configure terminal
Switch(config)# no ipv6 mld snooping vlan 10 querier address

Related Commands

show ipv6 mld snooping querier vlan

9.3.17 ipv6 mld snooping vlan querier-timeout

Command Purpose

Use this command to set mld previous querier timeout interval on this vlan. To reset it to default, use the no form of this command.

Command Syntax

ipv6 mld snooping vlan VLAN_ID querier-timeout INTERVAL
no ipv6 mld snooping vlan VLAN_ID querier-timeout
### Command Mode
Global Configuration

### Default
255s

### Usage
None

### Examples
This example shows how to set previous querier timeout interval as 100 seconds on vlan 10:

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 10 querier address 2001::2
```

This example shows how to reset previous querier timeout interval on vlan 10:

```
Switch# configure terminal
Switch(config)# no ipv6 mld snooping vlan 10 querier-timeout
```

### Related Commands
show ipv6 mld snooping querier vlan

### Command Purpose
Use this command to add static mld group on this vlan. To remove this setting, use the no form of this command.

### Command Syntax
```
ipv6 mld snooping vlan VLAN_ID static-group GRP_IPV6_ADDR ( source SRC_IPV6_ADDR | ) interface IFNAME
no ipv6 mld snooping vlan VLAN_ID static-group GRP_IPV6_ADDR ( source SRC_IPV6_ADDR | ) interface IFNAME
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>INTERVAL</td>
<td>The mld previous querier timeout interval on this VLAN (seconds)</td>
<td>60-300</td>
</tr>
<tr>
<td>GRP_IPV6_ADDR</td>
<td>The address of group configured on the specified interface.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>SRC_IPV6_ADDR</td>
<td>The address of source configured on the specified interface.</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>IFNAME</td>
<td>The interface configured as a member of specified group on this vlan</td>
<td>Support physical/aggregation ports</td>
</tr>
</tbody>
</table>
Default
None

Usage
None

Examples

This example shows how to add group ff0e::1234 on interface eth-0-11 of vlan 10:

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 10 querier-timeout 100
```

This example shows how to remove group ff0e::1234 from interface eth-0-11 of vlan 10:

```
Switch# configure terminal
Switch(config)# no ipv6 mld snooping vlan 10 static-group ff0e::1234 interface eth-0-11
```

Related Commands

show ipv6 mld snooping group

9.3.19 clear ipv6 mld snooping group

Command Purpose

Use this command to clear all mld snooping groups.

Command Syntax

clear ipv6 mld snooping ( group * )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>All multicast group address</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default
None

Usage
None
Examples

This example shows how to clear mld snooping group all:

Switch# clear ipv6 mld snooping

Related Commands

None

9.3.20 clear ipv6 mld snooping vlan group

Command Purpose

Use this command to clear mld snooping groups on vlan.

Command Syntax

clear ipv6 mld snooping vlan VLAN_ID

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to clear mld snooping group on vlan 10:

Switch# clear ipv6 mld snooping vlan 10

Related Commands

None
9.3.21  show ipv6 mld snooping global

**Command Purpose**

Use this command to show the global configurations of mld snooping.

**Command Syntax**

show ipv6 mld snooping global

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

This example shows how to display the global configurations of mld snooping:

```
Switch# show ipv6 mld snooping global
```

<table>
<thead>
<tr>
<th>Global Mld Snooping Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mld Snooping                                    :Enabled</td>
</tr>
<tr>
<td>Mld Snooping Fast-Leave                         :Disabled</td>
</tr>
<tr>
<td>Mld Snooping Version                            :1</td>
</tr>
<tr>
<td>Mld Snooping Max-Member-Number                  :4096</td>
</tr>
<tr>
<td>Mld Snooping Unknown Multicast Behavior          :Flood</td>
</tr>
<tr>
<td>Mld Snooping Report-Suppression                 :Enabled</td>
</tr>
</tbody>
</table>

**Related Commands**

None
9.3.22 show ipv6 mld snooping groups

Command Purpose

Use this command to show the mld snooping groups.

Command Syntax

show ipv6 mld snooping groups

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display mld snooping groups:

```
Switch# show ipv6 mld snooping groups
VLAN Interface   Group Address        Uptime    Expire-time
1    eth-0-3  ff0e:2111:1111:1111:1111:1111:1234:5678 00:00:04  00:04:16
```

Related Commands

None

9.3.23 show ipv6 mld snooping groups vlan

Command Purpose

Use this command to show the mld snooping groups on vlan.

Command Syntax

show ipv6 mld snooping groups vlan VLAN_ID (group_address | )
Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display mld snooping groups on vlan 1:

Switch# show ipv6 mld snooping groups vlan 1

MLD Snooping groups for vlan1
Interface: eth-0-3
Uptime: 00:00:42
Group mode: Exclude (Expires: 00:03:38)
Source list is empty

Related Commands

None

9.3.24 show ipv6 mld snooping groups count

Command Purpose

Use this command to show the mld snooping groups number.

Command Syntax

show ipv6 mld snooping groups (vlan VLAN_ID) count

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC
Default

None

Usage

None

Examples

This example shows how to display mld snooping groups number on vlan 1:

```
Switch# show ipv6 mld snooping groups vlan 1 count
Dynamic multicast groups count: 1
Static multicast groups count: 0
Total multicast groups count: 1
```

Related Commands

None

9.3.25 show ipv6 mld snooping querier

Command Purpose

Use this command to show the configurations of mld snooping querier information.

Command Syntax

```
show ipv6 mld snooping querier ( vlan VLAN_ID )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None
Examples

This example shows how to display the configurations of mld snooping querier on vlan 1:

Switch# show ipv6 mld snooping querier vlan 1

Global Mld Snooping Querier Configuration
-------------------------------------------------
Version :1
Last-Member-Query-Interval (msec) :1000
Max-Query-Response-Time (sec) :10
Query-Interval (sec) :125
Global Source-Address ::
TCN Query Count :2
TCN Query Interval (sec) :10
Vlan 1: MLD snooping querier status
--------------------------------------------
Elected querier is ::
--------------------------------------------
Admin state :Disabled
Admin version :1
Operational state :Non-Querier
Querier operational address ::
Querier configure address :N/A
Last-Member-Query-Interval (msec) :1000
Max-Query-Response-Time (sec) :10
Query-Interval (sec) :125
Querier-Timeout (sec) :255

Related Commands

None

9.3.26 show ipv6 mld snooping mrouter

Command Purpose

Use this command to show the information of mld snooping mrouter port on vlan.

Command Syntax

show ipv6 mld snooping mrouter ( vlan VLAN_ID | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>
Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the information of mld snooping mrouter port on vlan 1:

Switch# show ipv6 mld snooping mrouter  vlan 1

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Interface</th>
<th>Mode</th>
<th>Uptime</th>
<th>Expires-time</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>eth-0-1</td>
<td>static</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Related Commands

None

9.3.27  show ipv6 mld snooping vlan

Command Purpose

Use this command to show the configurations of mld snooping on vlan.

Command Syntax

show ipv6 mld snooping ( vlan VLAN_ID | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None
Usage

None

Examples

This example shows how to display the configurations of mld snooping on vlan 1:

Switch# show ipv6 mld snooping vlan 1

Global Mld Snooping Configuration
-------------------------------------
Mld Snooping :Enabled
Mld Snooping Fast-Leave :Disabled
Mld Snooping Version :1
Mld Snooping Max-Member-Number :4096
Mld Snooping Unknown Multicast Behavior :Flood
Mld Snooping Report-Suppression :Enabled

Vlan 2
--------
Mld Snooping :Enabled
Mld Snooping Fast-Leave :Disabled
Mld Snooping Report-Suppression :Enabled
Mld Snooping Version :1
Mld Snooping Max-Member-Number :4096
Mld Snooping Unknown Multicast Behavior :Flood
Mld Snooping Group Access-list :N/A
Mld Snooping Mrouter Port :eth-0-1(static)
Mld Snooping Mrouter Port Aging Interval(sec) :255

Related Commands

None

9.3.28  show resource l2mcast

Command Purpose

Use this command to display the resource usage of L2 mcast.

Command Syntax

show resource l2mcast
 Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show resource l2mcast command:

```
Switch# show resource l2mcast
L2MCAST
Resource    Used  Capability
----------------------------------------------
L2 Mcast Entry  1     1024
L2 Mcast Member  2      8192
```

Related Commands

None

9.4 PIMv6 Commands

9.4.1 ipv6 pim accept-register

Command Purpose

Use this command to apply an access-list to limit the ipv6 pim register message received by rp.

To remove this setting, use the no form of this command.

Command Syntax

```
ipv6 pim accept-register list LISTNAME
no ipv6 pim accept-register
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISTNAME</td>
<td>The name of the access-list to be applied.</td>
<td>A string with 1-20 characters</td>
</tr>
</tbody>
</table>
Command Mode

Global Configuration

Default

None

Usage

This feature is used to prevent the unauthorized user registered to the switch. When enable this feature, the system will send back a register stop message when the unauthorized register message is received.

Examples

This example shows how to apply the access-list acl1 to limit the ipv6 pim register message received by rp:

<table>
<thead>
<tr>
<th>Switch# configure terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# ipv6 pim accept-register list acl1</td>
</tr>
</tbody>
</table>

This example shows how to remove the limits:

<table>
<thead>
<tr>
<th>Switch# configure terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# no ipv6 pim accept-register</td>
</tr>
</tbody>
</table>

Related Commands

None

9.4.2 ipv6 pim anycast-rp

Command Purpose

Use this command to set anycast rendezvous-point. To remove the configurations, use the no form of this command.

Command Syntax

ipv6 pim anycast-rp ANYCAST_RP_ADDR ANYCAST_MEMBER_ADDR
no ipv6 pim anycast-rp ANYCAST_RP_ADDR (ANYCAST_MEMBER_ADDR )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANYCAST_RP_ADDR</td>
<td>Anycast rp address</td>
<td>IPv6 address</td>
</tr>
<tr>
<td>IPv6 address</td>
<td>IPv6 address</td>
<td>IPv6 address</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration
### Default

None

### Usage

Should configure every router in the network, and must configure same RP address.

### Examples

This example shows how to set anycast rendezvous-point:

```
Switch# configure terminal
Switch(config)# ipv6 pim anycast-rp 2001::2 2001::10
```

This example shows how to remove the member in anycast rendezvous-point:

```
Switch# configure terminal
Switch(config)# no ipv6 pim anycast-rp 2001::2 2001::10
```

### Related Commands

None

#### 9.4.3 `ipv6 pim bsr-candidate`

### Command Purpose

Use this command to configure the candidate bootstrap router (candidate BSR).

To remove the configurations, use the no form of this command.

### Command Syntax

```
ipv6 pim bsr-candidate IFNAME { HASH_MASK ( PRIORITY ) } |
no ipv6 pim bsr-candidate
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
<tr>
<td>HASH_MASK</td>
<td>Hash mask length for RP selection</td>
<td>0-128</td>
</tr>
<tr>
<td>PRIORITY</td>
<td>Priority value for candidate bootstrap router</td>
<td>0-255</td>
</tr>
</tbody>
</table>

### Command Mode

Global Configuration

### Default

None
Usage
None

Examples
This example shows how to configure the candidate BSR:
Switch# configure terminal
Switch(config)# ipv6 pim bsr-candidate eth-0-1

This example shows how to cancel the candidate BSR configured:
Switch# configure terminal
Switch(config)# no ipv6 pim bsr-candidate

Related Commands
ipv6 pim bsr-border

9.4.4 ipv6 pim bsr-border

Command Purpose
Use this command to configure the border of pim domain.
To remove the configurations of the border of pim domain, use the no form of this command.

Command Syntax
ipv6 pim bsr-border
no ipv6 pim bsr-border

Command Mode
Interface Configuration

Default
None

Usage
None

Examples
This example shows how to configure the border of pim domain:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 pim bsr-border

This example shows how to remove the configurations of the border of pim domain:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ipv6 pim bsr-border
Related Commands

ipv6 pim bsr-candidate

9.4.5 ipv6 pim dr-priority

Command Purpose

Use this command to configure the DR priority.
To return it to default value, use the no form of this command.

Command Syntax

ipv6 pim dr-priority PRIORITY

no ipv6 pim dr-priority

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRIORITY</td>
<td>The DR priority</td>
<td>0-4294967294</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

1

Usage

When a hello message without DR priority is received, it will be regarded to have the max DR priority and to be elected as DR. When more than one router’s hello messages do not have DR priority, the one which have the highest ipv6 address will be elected as DR.

Examples

This example shows how to set the pim router DR priority to 1000:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 pim dr-priority 1000

This example shows how to return the pim router DR priority to default value:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ipv6 pim dr-priority
Related Commands

None

9.4.6 ipv6 pim exclude-genid

Command Purpose

Use this command to exclude generation id option from pim hello packets on this interface.
To return to the default setting, use the no form of this command.

Command Syntax

ipv6 pim exclude-genid
no ipv6 pim exclude-genid

Command Mode

Interface Configuration

Default

Disable

Usage

GenerationID is the ID of a PIM neighbour, it is carried in PIM hello message, the receiver device will record every received GenerationID in the hello packet and check if GenerationID has changed, if GenerationID changed, will consider neighbour state changed and restart state machine.

Examples

This example shows how to exclude generation id option from pim hello packets on this interface:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 pim exclude-genid

This example shows how to return the generation id option to the default setting:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ipv6 pim exclude-genid

Related Commands

None
9.4.7 ipv6 pim hello-interval

**Command Purpose**

Use this command to configure the interval for pim hello packets on this interface. To reset to the default setting, use the no form of this command.

**Command Syntax**

ipv6 pim hello-interval INTERVAL
no ipv6 pim hello-interval

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>The pim hello message interval (second)</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

30s

**Usage**

None

**Examples**

This example shows how to set the pim hello message interval to 100s:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 pim hello-interval 100
```

This example shows how to reset the pim hello message interval to default value:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ipv6 pim hello-interval
```

**Related Commands**

None
9.4.8 ipv6 pim ignore-rp-set-priority

Command Purpose

Use this command to ignore RP set priority value.
To not ignore the priority, use the no form of this command.

Command Syntax

ipv6 pim ignore-rp-set-priority
no ipv6 pim ignore-rp-set-priority

Command Mode

Global Configuration

Default

Not ignore RP set priority value.

Usage

None

Examples

This example shows how to ignore RP set priority value:
Switch# configure terminal
Switch(config)# ipv6 pim ignore-rp-set-priority

This example shows how to return the configurations to default value:
Switch# configure terminal
Switch(config)# no ipv6 pim ignore-rp-set-priority

Related Commands

None

9.4.9 ipv6 pim jp-timer

Command Purpose

Use this command to set the join/prune timer value.
To return the timer to default value, use the no form of this command.
Command Syntax

ipv6 pim jp-timer SECOND
no ipv6 pim jp-timer

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECOND</td>
<td>The Join/Prune timer value (second)</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

60s

Usage

None

Examples

This example shows how to set the join/prune timer value to 100s:

Switch# configure terminal
Switch(config)# ipv6 pim jp-timer 100

This example shows how to return the join/prune timer value to default value:

Switch# configure terminal
Switch(config)# no ipv6 pim jp-timer

Related Commands

None

9.4.10 ipv6 pim neighbor-filter

Command Purpose

Use this command to add an access-list to filter the neighbor.
To remove this filter, use the no form of this command.

Command Syntax

ipv6 pim neighbor-filter LISTNAME
no ipv6 pim neighbor-filter
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISTNAME</td>
<td>The name of the access-list</td>
<td>A string with 1-20 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

None

**Usage**

Neighbours would send hello message to each other to establish connections with other neighbour. You can use this command to filter which neighbour can be connected or not.

**Examples**

This example shows how to establish neighbors based on access-list acl1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 pim neighbor-filter acl1
```

This example shows how to cancel the filter:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ipv6 pim neighbor-filter
```

**Related Commands**

None

**9.4.11 ipv6 pim register-rate-limit**

**Command Purpose**

Use this command to set the rate limit for pim registers. To return the rate limit to default value, use the no form of this command.

**Command Syntax**

ipv6 pim register-rate-limit LIMIT
no ipv6 pim register-rate-limit
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIMIT</td>
<td>The rate limit for pim registers send from DR to RP</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

By default, will not limit PIM register messages, if a limit is set, PIM register messages will be discard when packet reached by this limit.

**Usage**

There is no rate limit for pim registers by default.
When the rate limit is configured, the exceed pim register message will be dropped on the rp.

**Examples**

This example shows how to set the rate limit for pim registers to 100 per second:

```
Switch# configure terminal
Switch(config)# ipv6 pim register-rate-limit 100
```

This example shows how to cancel the rate limit:

```
Switch# configure terminal
Switch(config)# no ipv6 pim register-rate-limit
```

**Related Commands**

ipv6 pim register-rp-reachability
ipv6 pim register-source
ipv6 pim register-suppression

**9.4.12 ipv6 pim register-source**

**Command Purpose**

Use this command to set the source address for pim register.
To return the source address for pim register to default value, use the no form of this command.

**Command Syntax**

ipv6 pim register-source IFNAME
no ipv6 pim register-source
### Command Mode

**Global Configuration**

**Default**

The source address for pim register is the interface ipv6 address of dr by default.

**Usage**

None

**Examples**

This example shows how to set the source address for pim register to the ipv6 address of interface eth-0-1:

```
Switch# configure terminal
Switch(config)# ipv6 pim register-source eth-0-1
```

This example shows how to return the source address for pim register to default value:

```
Switch# configure terminal
Switch(config)# no ipv6 pim register-source
```

**Related Commands**

- `ipv6 pim register-rate-limit`
- `ipv6 pim register-rp-reachability`
- `ipv6 pim register-suppression`

---

### 9.4.13 ipv6 pim register-rp-reachability

**Command Purpose**

Use this command to enable rp reachability check for pim registers.
To disable this check, use the no form of this command.

**Command Syntax**

- `ipv6 pim register-rp-reachability`
- `no ipv6 pim register-rp-reachability`
**Command Mode**

Global Configuration

**Default**

Disable.

**Usage**

None

**Examples**

This example shows how to enable rp reachability check for pim registers:

```
Switch# configure terminal
Switch(config)#ipv6 pim register-rp-reachability
```

This example shows how to disable rp reachability check for pim registers:

```
Switch# configure terminal
Switch(config)#no ipv6 pim register-rp-reachability
```

**Related Commands**

ipv6 pim register-rate-limit
ipv6 pim register-source

**9.4.14 ipv6 pim register-suppression**

**Command Purpose**

Use this command to set the register suppression time.

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

**Command Syntax**

```
ipv6 pim register-suppression SECOND
no ipv6 pim register-suppression
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECOND</td>
<td>The register suppression time in seconds</td>
<td>11-65535</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration
**Default**

60s

**Usage**

None

**Examples**

This example shows how to set the register suppression time to 100s:

Switch# configure terminal
Switch(config)# ipv6 pim register-suppression 100

This example shows how to return the register suppression time to default value:

Switch# configure terminal
Switch(config)# no ipv6 pim register-suppression

**Related Commands**

ipv6 pim register-rate-limit
ipv6 pim register-rp-reachability
ipv6 pim register-source

**9.4.15 ipv6 pim rp-address**

**Command Purpose**

Use this command to set the ipv6 pim rp (rendezvous point) address.
To remove it, use the no form of this command.

**Command Syntax**

ipv6 pim rp-address IPV6_ADDR (LISTNAME | override | )
no ipv6 pim rp-address IPV6_ADDR (LISTNAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPV6_ADDR</td>
<td>The rp address</td>
<td>IPv6 address</td>
</tr>
<tr>
<td>LISTNAME</td>
<td>The name of an access-list</td>
<td>A string with 1-20 characters</td>
</tr>
<tr>
<td>override</td>
<td>Overrides dynamically learned RP mappings</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration
Default
None

Usage
None

Examples

This example shows how to set the pim rp address to 2001::2:
Switch# configure terminal
Switch(config)# ipv6 pim rp-address 2001::2

This example shows how to remove the rp address 2001::2:
Switch# configure terminal
Switch(config)# no ipv6 pim rp-address 2001::2

Related Commands
ipv6 pim rp-candidate
ipv6 pim rp-register-kat

9.4.16 ipv6 pim rp-candidate

Command Purpose

Use this command to set the candidate rp.
To remove the candidate rp, use the no form of this command.

Command Syntax

ipv6 pim rp-candidate IFNAME ( { priority PRIORITY | interval INTERVAL | group-list LISTNAME } )
no ipv6 pim rp-candidate ( IFNAME )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>The name of the interface to be the candidate rp</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
<tr>
<td>PRIORITY</td>
<td>The Candidate-RP priority</td>
<td>0-255</td>
</tr>
<tr>
<td>INTERVAL</td>
<td>The C-RP advertisement interval in seconds</td>
<td>1-16383</td>
</tr>
<tr>
<td>LISTNAME</td>
<td>Group ranges for this C-RP, only permit filters would be cared</td>
<td>A string with 1-20 characters</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration
Default
None

Usage
None

Examples
This example shows how to set the interface eth-0-1 to be the candidate rp:
Switch# configure terminal
Switch(config)# ipv6 pim rp-candidate eth-0-1
This example shows how to cancel the configured candidate rp:
Switch# configure terminal
Switch(config)# no ipv6 pim rp-candidate eth-0-1

Related Commands
ipv6 pim rp-address

9.4.17 ipv6 pim rp-register-kat

Command Purpose
Use this command to set the keepalive timer (KAT) for (S,G) at RP from PIM registers.
To return this timer to default value, use the no form of this command.

Command Syntax
ipv6 pim rp-register-kat SECOND
no ipv6 pim rp-register-kat

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECOND</td>
<td>The KAT time in seconds</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
185s
Usage

The register message send from dr will add an entry on rp. This entry will be aged when the keepalive timer expired which can be configured by this command.

Examples

This example shows how to set the keepalive timer to 100s at RP from PIM registers:

```
Switch# configure terminal
Switch(config)# ipv6 pim rp-register-kat 100
```

This example shows how to return this timer to default value:

```
Switch# configure terminal
Switch(config)# no ipv6 pim rp-register-kat
```

Related Commands

ipv6 pim rp-address
ipv6 pim rp-candidate

9.4.18 ipv6 pim spt-switch-threshold infinity

Command Purpose

Use this command to set the spt switch threshold to infinity.
To cancel this setting, use the no form of this command.

Command Syntax

```
ipv6 pim spt-switch-threshold infinity { group-list LISTNAME | }
no ipv6 pim spt-switch-threshold infinity { group-list LISTNAME | }
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISTNAME</td>
<td>Group address access list</td>
<td>A string with 1-20 characters</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

The DR will switch to spt immediately when received the first multicast packet by default.

Usage

None
Examples
This example shows how to set the spt switch threshold to infinity:

Switch# configure terminal
Switch(config)# ipv6 pim spt-switch-threshold infinity

This example shows how to return the spt-switch-threshold to default:

Switch# configure terminal
Switch(config)# no ipv6 pim spt-switch-threshold infinity

Related Commands
show ipv6 pim sparse-mode spt-threshold

9.4.19  ipv6 pim cisco-register-checksum

Command Purpose
Use this command to calculate register checksum over whole packet (cisco compatibility).
To remove this setting, use the no form of this command.

Command Syntax
ipv6 pim cisco-register-checksum ( group-list LISTNAME | )
no ipv6 pim cisco-register-checksum ( group-list LISTNAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISTNAME</td>
<td>Group address access list</td>
<td>A string with 1-20 characters</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
The register checksum defined in RFC is used by default.

Usage
The register checksum defined in RFC is used by default, if group-list is configured, only packets that verified can be sent in CISCO way.

Examples
This example shows how to set to calculate register checksum over whole packet:

Switch# configure terminal
Switch(config)# ipv6 pim cisco-register-checksum

This example shows how to remove this setting:

Switch# configure terminal
Switch(config)# no ipv6 pim cisco-register-checksum

Related Commands
None
9.4.20 ipv6 pim sparse-mode

**Command Purpose**

Use this command to enable pim sparse mode on the interface.
To disable pim sparse mode, use the no form of this command.

**Command Syntax**

```
ipv6 pim sparse-mode (passive | )
no ipv6 pim sparse-mode (passive | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>passive</td>
<td>Pim passive mode (local members only)</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

Disable

**Usage**

The pim hello message will not be sent out from the interface when the passive mode is configured.

**Examples**

This example shows how to enable pim sparse mode on the interface:
```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 pim sparse-mode
```

This example shows how to disable pim sparse mode on the interface:
```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ipv6 pim sparse-mode
```

This example shows how to enable pim sparse mode passive on the interface:
```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 pim sparse-mode passive
```

**Related Commands**

None
9.4.21 ipv6 pim unicast-bsm

Command Purpose

Use this command to enable sending and receiving of unicast BSM for backward compatibility. To cancel this setting, use the no form of this command.

Command Syntax

ipv6 pim unicast-bsm
no ipv6 pim unicast-bsm

Command Mode

Interface Configuration

Default

Disable

Usage

Interface will send BSM message to the whole pim domain by default.

Examples

This example shows how to enable sending and receiving of unicast BSM for backward compatibility:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 pim unicast-bsm

This example shows how to cancel this setting:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ipv6 pim unicast-bsm

Related Commands

None

9.4.22 ipv6 pim ssm

Command Purpose

Use this command to enable pim-ssm and set ssm group range. To cancel this setting, use the no form of this command.
Command Syntax

ipv6 pim ssm (default | range LISTNAME)
no ipv6 pim ssm

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Use FF3x::/32 group range for SSM</td>
<td>-</td>
</tr>
<tr>
<td>LISTNAME</td>
<td>ACL for group range to be used for SSM</td>
<td>A string with 1-20 characters</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

Disable

Usage

Enable pim-ssm and set ssm group range.

Examples

This example shows how to enable pim-ssm and set ssm group range to default:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 pim ssm default

This example shows how to cancel this setting:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ipv6 pim ssm default

Related Commands
None

9.4.23 show ipv6 pim sparse-mode bsr-router

Command Purpose

Use this command to show the information of bootstrap router.

Command Syntax

show ipv6 pim sparse-mode bsr-router
Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the information of bootstrap router:

Switch# show ipv6 pim sparse-mode bsr-router

PIM6v2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 2001:2::1 (?)
  Uptime: 00:00:08, BSR Priority: 64, Hash mask length: 126
  Next bootstrap message in 00:00:52
  Role: Candidate BSR
  State: Elected BSR

Related Commands

None

9.4.24  show ipv6 pim sparse-mode interface

Command Purpose

Use this command to show the information of pim interface.

Command Syntax

show ipv6 pim sparse-mode interface ( detail | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Detailed interface information</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC
**Default**
None

**Usage**
None

**Examples**
This example shows how to display the information of pim interface:

```
Switch# show ipv6 pim sparse-mode interface detail
eth-0-1 (vif 0):
  Address fe80::9c7c:7eff:fe94:8300, DR fe80::9c7c:7eff:fe94:8300
  Hello period 30 seconds, Next Hello in 3 seconds
  Triggered Hello period 5 seconds
  Secondary addresses:
      2001:1::1
  Neighbors:
```

**Related Commands**
None

**9.4.25 show ipv6 pim sparse-mode local-member**

**Command Purpose**
Use this command to show the pim local membership information.

**Command Syntax**
```
show ipv6 pim sparse-mode local-member (IFNAME | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None
Examples
This example shows how to display PIM local membership information:

Switch# show ipv6 pim sparse-mode local-members

PIM Local membership information
eth-0-2:
*, ff0e::1234:5678
  info: Include

Related Commands
None

9.4.26 show ipv6 pim sparse-mode mroute

Command Purpose
Use this command to show the mroute information of PIM sparse mode.

Command Syntax
show ipv6 pim sparse-mode mroute { SRC_IPV6_ADDR | GROUP_IPV6_ADDR } [ detail ]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRC_IPV6_ADDR</td>
<td>Source address</td>
<td>IPv6 address</td>
</tr>
<tr>
<td>GROUP_IPV6_ADDR</td>
<td>Group address</td>
<td>IPv6 address</td>
</tr>
<tr>
<td>detail</td>
<td>Detailed interface information</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to display PIM mroute information:

Switch# show ipv6 pim sparse-mode mroute detail

IPv6 Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0
*, ff0e::1234:5678
Type: (*,G)
Uptime: 00:01:49
  RP: None, RPF nbr: None, RPF idx: None
Upstream:
  State: JOINED, SPT Switch: Enabled, JT: off
  Macro state: Join Desired,
Downstream:
  eth-0-2:
    State: NO INFO, ET: off, PPT: off
    Assert State: NO INFO, AT: off
    Winner: None, Metric: 4294967295, Pref: 4294967295, RPT bit: on
    Macro state: Could Assert, Assert Track
Local Olist:
  eth-0-2

Related Commands
None

9.4.27 show ipv6 pim sparse-mode neighbor

Command Purpose
Use this command to show the neighbor information of pim sparse mode.

Command Syntax
show ipv6 pim sparse-mode neighbor ( IFNAME ( IPV6_ADDR | detail | ) | detail | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
<tr>
<td>IPV6_ADDR</td>
<td>Neighbor address</td>
<td>IPv6 address</td>
</tr>
<tr>
<td>detail</td>
<td></td>
<td>Detailed interface information</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None
Examples

This example shows how to display the neighbor information of pim sparse mode:

Switch# show ipv6 pim sparse-mode neighbor

<table>
<thead>
<tr>
<th>Neighbor Address</th>
<th>Interface</th>
<th>Uptime/Expires</th>
<th>DR Pri/Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe80::9c7c:7eff:fe94:8300</td>
<td>eth-0-9</td>
<td>00:00:40/00:01:44</td>
<td>1 DR</td>
</tr>
</tbody>
</table>

Related Commands

None

9.4.28 show ipv6 pim sparse-mode rp mapping

Command Purpose

Use this command to show group to rp mappings.

Command Syntax

show ipv6 pim sparse-mode rp mapping

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display group to rp mappings:

Switch# show ipv6 pim sparse-mode rp mapping

RP: 2001::1
Info source: 2001::1, via bootstrap
Related Commands

None

9.4.29 show ipv6 pim sparse-mode rp-hash

Command Purpose

Use this command to show the information of rp to be chosen based on group selected.

Command Syntax

show ipv6 pim sparse-mode rp-hash GROUP_IPV6_ADDR

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_IPV6_ADDR</td>
<td>Multicast group address</td>
<td>IPv6 address</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the information of rp to be chosen based on group ff02::1234:

Switch# show ipv6 pim sparse-mode rp-hash ff02::1234

RP: 2001::2

Related Commands

None
9.4.30 show ipv6 pim sparse-mode spt-threshold

Command Purpose

Use this command to show the rpt to spt threshold of pim sparse mode.

Command Syntax

show ipv6 pim sparse-mode spt-threshold

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the rpt to spt threshold of pim sparse mode:

Switch# show ipv6 pim sparse-mode spt-threshold

IPv6 PIM spare-mode immediately switches over to SPT upon receiving the first traffic

Related Commands

None

9.5 MVR6 Commands

9.5.1 mvr6

Command Purpose

Use this command to enable or disable MVR6. To disable mvr6, use the no form of this command.

Command Syntax

mvr6

no mvr6
**Command Mode**

Global Configuration

**Default**

Disable

**Usage**

Enable MVR6 in the Switch, must disable ipv6 multicast-routing before enable MVR6.

**Examples**

This example shows how to enable MVR6:

```
Switch# configure terminal
Switch(config)# no ipv6 multicast-routing
Switch(config)# mvr6
```

**Related Commands**

show mvr6

9.5.2 mvr6 vlan

**Command Purpose**

Use this command to specify the MVR6 source vlan. To remove this setting, use the no form of this command.

**Command Syntax**

```
mvr6 vlan VLAN_ID
no mvr6 vlan
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

None
Usage

The related vlan interface should be created before the configuration of the MVR6 source vlan.

Examples

This example shows how to configure source vlan of MVR6. configure vlan 2 as source vlan of MVR6:

Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config)# interface vlan 2
Switch(config-if)# exit
Switch(config)# mvr6 vlan 2

Related Commands

interface vlan

9.5.3 mvr6 group

Command Purpose

Use this command to configure global group for MVR6. To remove this setting, use the no form of this command.

Command Syntax

mvr6 group IPV6_ADDR ( COUNT )
no mvr6 group address ( COUNT )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPV6_ADDR</td>
<td>Multicast group address</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>COUNT</td>
<td>Count of contiguous groups</td>
<td>1-64</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

This command is used to create or delete a global static group.
Examples

This example shows how to create global static group from ff0e::1 to ff0e::50:

<table>
<thead>
<tr>
<th>Switch#</th>
<th>configure terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)#</td>
<td>mvr6 group ff0e::1 50</td>
</tr>
</tbody>
</table>

Related Commands

None

9.5.4 mvr6 source-address

Command Purpose

Use this command to create mvr6 source address. To reset it to default value, use the no form of this command.

Command Syntax

mvr6 source-address IPv6_ADDR

no mvr6 source-address

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6_ADDR</td>
<td>Source ipv6 address</td>
<td>IPv6 Address</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

fe80::1

Usage

None

Examples

This example shows how to create mvr6 source address:

<table>
<thead>
<tr>
<th>Switch#</th>
<th>configure terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)#</td>
<td>mvr6 source-address 2001::2</td>
</tr>
</tbody>
</table>

This example shows how to resume mvr6 source address as default IPv6 address:

<table>
<thead>
<tr>
<th>Switch#</th>
<th>configure terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)#</td>
<td>no mvr6 source-address</td>
</tr>
</tbody>
</table>
9.5.5  mvr6 type

Command Purpose

Use this command to configure a switch-port as source port or receiver port. To remove this setting, use the no form of this command.

Command Syntax

mvr6 type ( source | receiver vlan VLAN_ID )
no mvr6 type ( receiver vlan VLAN_ID | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>MVR6 source port</td>
<td>-</td>
</tr>
<tr>
<td>receiver</td>
<td>MVR6 receiver port</td>
<td>-</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>MVR6 receiver vlan</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

None

Usage

Configure the interface as source port or receiver port. The source port must belong to source vlan, and the receiver port must not belong to source vlan.

Examples

This example shows how to configure the eth-0-1 as source port, and configure the eth-0-2 as receiver port of vlan 2:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# mvr6 type source
Switch(config-if)# interface eth-0-2
Switch(config-if)# mvr6 type receiver vlan 2
```

Related Commands

None
9.5.6 show mvr6

Command Purpose

Use this command to show mvr6 information.

Command Syntax

show mvr6

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display mrv6 information:

Switch# show mvr6

MVR6 Running: TRUE
MVR6 Multicast VLAN: 2
MVR6 Source-address: fe80::1
MVR6 Max Multicast Groups: 1024
MVR6 Hw Rt Limit: 224
MVR6 Current Multicast Groups: 3

Related Commands

None

9.5.7 show mvr6 interface

Command Purpose

Use this command to show mvr6 interface information.
Command Syntax

show mvr6 interface

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display mvr6 interface information:

```
Switch# show mvr6 interface

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>VLAN</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-0-2</td>
<td>source</td>
<td>10</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>eth-0-1</td>
<td>receiver</td>
<td>11</td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>
```

Related Commands

None

9.5.8 show mvr6 group

Command Purpose

Use this command to show mvr6 group learned from receiver port.

Command Syntax

show mvr6 group vlan VLAN_ID (IPV6_ADDR )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>MVR6 receiver VLAN</td>
<td>1-4094</td>
</tr>
<tr>
<td>IPV6_ADDR</td>
<td>Multicast group address</td>
<td>IPv6 Address</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC
Default
None

Usage
None

Examples
This example shows how to display mvr6 group learned from receiver port:

Switch# show mvr6 groups

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Interface</th>
<th>Group Address</th>
<th>Uptime</th>
<th>Expire-time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>eth-0-3</td>
<td>ff0e:2111:1111:1111:1111:1234:5678</td>
<td>00:00:11</td>
<td>00:04:10</td>
</tr>
</tbody>
</table>

Related Commands
None

9.5.9 show mvr6 group static

Command Purpose
Use this command to show mvr6 global static groups.

Command Syntax
show mvr6 group static global

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to display mvr6 global static groups:

Switch# show mvr6 groups static global

MVR6 Static Global Group:
ff0e:1234
ff0e:1235
ff0e:1236
ff0e:2111:1111:1111:1111:1234:5678
Related Commands

None

9.5.10 show resource mvr6

Command Purpose

Use this command to display the resource usage of MVR6.

Command Syntax

show resource mvr6

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the resource usage of MVR6:

Switch# show resource mvr6

<table>
<thead>
<tr>
<th>MVR Resource</th>
<th>Used</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>MVR Entry</td>
<td>4</td>
<td>224</td>
</tr>
<tr>
<td>L2 Mcast Member</td>
<td>1</td>
<td>1792</td>
</tr>
</tbody>
</table>

Related Commands

None
Chapter 10 Traffic Management Commands

10.1 QOS Commands

10.1.1 class-map type qos

Command Purpose
To create or modify a class map and enter the class-map configuration mode, use the class-map command. To remove a class map, use the no form of this command.

Command Syntax

class-map type qos NAME

no class-map NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Name assigned to the class map. The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores. The name class-default is reserved.</td>
<td></td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
You can define a class map for each class of traffic to be used in QoS policies. If the packet matches any of the criteria configured for this class map with the match command, then this class map is applied to the packet. If no execution strategy is specified (match-any or match-all), then the default value of match-any is applied to the traffic class.

Examples

Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap-qos)# class type qos cmap_qos

Related Commands

class type qos
show class-map

10.1.2 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>access-list name</td>
<td>The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.</td>
</tr>
</tbody>
</table>

### Command Mode

Class-map Configuration

### Default

None

### Usage

None

### Examples

Switch# configure terminal
Switch(config)# class-map type qos cmap_qos
Switch(config-cmap-qos)# match access-group example

### Related Commands

10.1.3 match cos

### Command Purpose

To define the class of traffic using the class of service (CoS) value in class map, use the match cos command. To remove the match on the CoS value, use the no form of this command.

### Command Syntax

match cos [inner] COS

no match cos [inner] COS

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>COS</td>
<td>Specified CoS value</td>
<td>0-7</td>
</tr>
</tbody>
</table>

### Command Mode

Class-map Configuration

### Default

None

### Usage

None

### Examples

Switch# configure terminal
Switch(config)# class-map type qos cmap_qos
Switch(config-cmap-qos)# match cos 5

### Related Commands

10.1.4 match dscp

### Command Purpose

To identify specific differentiated services code point (DSCP) values as a match criterion, use the match dscp command. To remove specified DSCP values as a match criterion, use the no form of this command.
**Command Syntax**

match dscp DSCP_STR

no match dscp DSCP_STR

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP_STR</td>
<td>Specified DSCP value</td>
<td>0-63</td>
</tr>
</tbody>
</table>

**Command Mode**

Class-map Configuration

**Default**

None

**Usage**

Match criteria can be PHB string

**Examples**

Switch# configure terminal
Switch(config)# class-map type qos cmap_qos
Switch(config-cmap-qos)# match dscp af11

**Related Commands**

10.1.5 class-map type traffic-class

**Command Purpose**

To create or modify a class map and enter the class-map configuration mode, use the class-map command. To remove a class map, use the no form of this command.

**Command Syntax**

class-map type traffic-class NAME

no class-map NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Name assigned to the class map.</td>
<td>The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores. The name class-default is reserved.</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

None

**Usage**

This type class-map is used to identify traffic flows with different traffic class.

**Examples**

Switch# configure terminal
Switch(config)# class-map type traffic-class cmap_tc

**Related Commands**

class type traffic-class

show class-map
10.1.6 match traffic-class

Command Purpose
To configure a class map to use a specific QoS traffic-class value as a match criterion, use the match traffic-class command. To remove the specified protocol as match criteria, use the no form of this command.

Command Syntax
match traffic-class CLASS-ID
no match

```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
</table>
| CLASS-ID  | Specified traffic class value    | The valid values are from 1 to 7.
```

Command Mode
Class-map Configuration

Default
None

Usage
None

Examples
Switch# configure terminal
Switch(config)# class-map type traffic-class cmap_tc
Switch(config-cmap-tc)# match traffic-class 6

Related Commands
class-map

10.1.7 policy-map type qos

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

Command Syntax
policy-map type qos NAME
no policy-map NAME

```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Name assigned to the policy map.</td>
<td>The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.</td>
</tr>
</tbody>
</table>
```

Command Mode
Global Configuration

Default
None

Usage
The policy-map can be attached to multiple physical ports at ingress directions.
Examples
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos

Related Commands
service-policy type qos
show policy-map

10.1.8 class type qos

Command Purpose
To add a reference to an existing class map in a policy map and enter the class mode, use the class command. To remove a class from the policy map, use the no form of this command

Command Syntax
class type qos NAME
no class NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
</table>
| NAME      | Reference to a class map. | The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode
Policy-map Configuration

Default
None

Usage
Policy actions in the first class that matches the traffic type are performed.
By default, the class-default class is created under every policy map in the system. You cannot change this mapping.
You cannot remove the class-default. If you attempt to delete the class-default class, the switch returns an error message.

Examples
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap)# class type qos cmap1

Related Commands
policy-map type qos
class-map type qos

10.1.9 class type qos class-default

Command Purpose
To add a reference to the system default class that does not match any traffic class, use the class class-default command. To remove the system default class from the policy map, use the no form of this command.

Command Syntax
class type qos class-default
no class class-default
Command Mode
Policy-map Configuration

Default
None

Usage
Traffic that fails to match any class is assigned to a default class of traffic called class-default. You cannot delete this class.

Examples
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap-qos)# class type qos class-default

Related Commands
policy-map type qos

10.1.10 set cos

Command Purpose
Use this command to remark packet CoS value.

Command Syntax
set cos { [ inner ] COS | cos table NAME | dscp table NAME }
no set cos { [ inner ] COS | cos table NAME | dscp table NAME }

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>COS</td>
<td>CoS value</td>
<td>range 0-7</td>
</tr>
<tr>
<td>NAME</td>
<td>Reference to a mutation map</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Config-pmap-c Configuration

Default
Disabled

Usage
There are four ways to set cos. Each way can only be reset by its no command while "no set cos" command can reset all ways. "no set cos COS" command do not care COS value.

Examples
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap-qos)# class type qos cmap_qos
Switch(config-pmap-qos-c)# set cos 3

Related Commands
10.1.11  set dscp

Command Purpose

Use this command to mark DSCP value.

Command Syntax

set dscp { DSCP | PHB_STR | default | dscp table NAME | cos table NAME }

no set dscp { DSCP | PHB_STR | default | dscp table NAME | cos table NAME }

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP</td>
<td>DSCP value</td>
<td>range 0-63</td>
</tr>
<tr>
<td>PHB_STR</td>
<td>PHB name</td>
<td>af11</td>
</tr>
<tr>
<td>default</td>
<td>default value (000000)</td>
<td>-</td>
</tr>
<tr>
<td>NAME</td>
<td>Reference to a mutation map</td>
<td>The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.</td>
</tr>
</tbody>
</table>

Command Mode

Config-pmap-c Configuration

Default

Disabled

Usage

There are three ways to set dscp. Each way can only be reset by its no command while "no set dscp" command can reset all ways.

"no set dscp DSCP" command do not care DSCP value.

Examples

Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap-qos)# class type qos cmap_qos
Switch(config-pmap-qos-c)# set dscp cs3

Related Commands

10.1.12  set traffic-class

Command Purpose

Use this command to set traffic flow's class ID.

Command Syntax

set traffic-class CLASS-ID

no set traffic-class

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLASS-ID</td>
<td>traffic class ID</td>
<td>range is 0-7</td>
</tr>
</tbody>
</table>

Command Mode

Config-pmap-c Configuration

Default

None
Usage
Traffic flow with different traffic class ID would be given varieties of treatments in ingress and egress. This command has higher priority with policer set traffic-class command.

Examples

```
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap-qos)# class type qos cmap_qos
Switch(config-pmap-qos-c)# set traffic-class 3
```

Related Commands

**10.1.13 set color**

**Command Purpose**
Use this command to set traffic flow’s color.

**Command Syntax**

```
set color { red | yellow }
```

```
no set color
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>red</td>
<td>red color</td>
<td>-</td>
</tr>
<tr>
<td>yellow</td>
<td>yellow color</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**
Config-pmap-c Configuration

**Default**
None

**Usage**
None

**Examples**

```
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap-qos)# class type qos cmap_qos
Switch(config-pmap-qos-c)# set color red
```

**Related Commands**

**10.1.14 aggregate-policer**

**Command Purpose**
Use this command to rate-limit the aggregate traffic matching this traffic class for all interfaces in the same slot. To cancel rate limit, use the no form of this command.

**Command Syntax**

```
aggregate-policer NAME
```

```
no aggregate-policer
```
### Aggregate policer

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Aggregate policer name.</td>
<td>The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.</td>
</tr>
</tbody>
</table>

**Command Mode**

Config-pmap-c Configuration

**Default**

Disabled

**Usage**

Policer and aggregate-policer cannot be set together in the same policy map. This command has lower priority with set traffic-class command.

**Examples**

```
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap-qos)# class type qos cmap_qos
Switch(config-pmap-qos-c)# aggregate-policer transmit
```

**Related Commands**

- qos aggregate-policer
- show qos aggregate policer

### policy-map type traffic-class

**Command Purpose**

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

**Command Syntax**

```
policy-map traffic-class NAME
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Specify a policy-map name</td>
<td>The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

Disabled

**Usage**

This command is used to create policy map to identify traffic flows with different traffic class.

**Examples**

```
Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
```

**Related Commands**

- service-policy traffic-class
10.1.16  class type traffic-class

Command Purpose
To add a reference to an existing class map in a policy map and enter the class mode, use the class command. To remove a class from the policy map, use the no form of this command.

Command Syntax
class type traffic-class NAME
no class NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Reference to a class map.</td>
<td>The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.</td>
</tr>
</tbody>
</table>

Command Mode
Policy-map Configuration

Default
None

Usage
Using this command, traffic classified by traffic-class can be specified varieties of properties, such as priority, bandwidth, etc.

Examples

Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
Switch(config-pmap-tc)# class type traffic-class cmap_tc

Related Commands
policy-map type traffic-class
class-map type traffic-class

10.1.17  class type traffic-class class-default

Command Purpose
To add a reference to an existing class map in a policy map and enter the class mode, use the class command. To remove a class from the policy map, use the no form of this command.

Command Syntax
class type traffic-class NAME
no class NAME

Command Mode
Policy-map Configuration

Default
None

Usage
Using this command, traffic classified by traffic-class can be specified varieties of properties, such as priority, bandwidth, etc.
Examples

Switch(config-pmap-tc-c)# priority level

10.1.18 priority level

Command Purpose
To assign a strict priority level to a traffic class in a policy map, use the priority level command. To remove the mapping, use the no form of this command.

Command Syntax

priority level LEVEL
no priority level

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LEVEL</td>
<td>Specifies the strict-priority level.</td>
<td>range 0-7</td>
</tr>
</tbody>
</table>

Command Mode

Config-pmap-c Configuration

Default

None

Usage

When the level is the same, queues will be scheduled on WDRR mode, otherwise will be scheduled on SP mode.

Examples

Switch(config-pmap-tc-c)# priority level

Related Commands

show qos interface egress

10.1.19 bandwidth percentage

Command Purpose
Use this command to allocate a percentage of the interface bandwidth to a queue. To remove configuration, use the no form of this command.

Command Syntax

bandwidth percentage PERCENTAGE
no bandwidth percentage
### Command Mode

**Config-pmap-c Configuration**

### Default

None

### Usage

Total percentage of all queues is 100. Unused bandwidth is allocated to default class.

### Examples

```bash
Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
Switch(config-pmap-tc)# class type traffic-class cmap_tc
Switch(config-pmap-tc-c)# bandwidth percentage 20
```

### Related Commands

- `show qos interface egress`

### 10.1.20 queue-limit

#### Command Purpose

Use this command to specify queue buffer.

#### Command Syntax

```
queue-limit SIZE [ecn-threshold THRESHOLD ]
```

```
no queue-limit
```

### Parameter Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERCENTAGE</td>
<td>Specifies the percentage of bandwidth of the underlying link rate.</td>
<td>The range is 1-100.</td>
</tr>
</tbody>
</table>

#### Command Mode

**Config-pmap-c Configuration**

#### Default

64 buffer cells for control traffic;

256 buffer cells for non-drop traffic.

#### Usage

Queue-limit, queue-limit dynamic and random-detect are conflict.

#### Examples

```bash
Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
Switch(config-pmap-tc)# class type traffic-class cmap_tc
Switch(config-pmap-tc-c)# queue-limit 200
```
Related Commands

show qos interface egress

10.1.21 queue-limit dynamic

Command Purpose

Use this command to specify dynamic buffer for queue.

Command Syntax

queue-limit dynamic LEVEL

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LEVEL</td>
<td>Queue level</td>
<td>range 0-10</td>
</tr>
</tbody>
</table>

Command Mode

Config-pmap-c Configuration

Default

10

Usage

Queue buffer can be caculated by the following expression:

\[ \text{threshold} = \left( \frac{f}{1+f} \right) \times \text{remainCnt} \quad (f = 1/128 \sim 8) \]

f mapping:

- level factor percent of remain buffer
- 0 1/128 ~0.8%
- 1 1/64 ~1.5%
- 2 1/32 ~3%
- 3 1/16 ~6%
- 4 1/8 ~11%
- 5 1/4 20%
- 6 1/2 ~33%
- 7 1 50%
- 8 2 ~66%
- 9 4 ~80%
- 10 8 ~89%

Queue-limit, queue-limit dynamic and random-detect are conflict.

Examples

Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
Switch(config-pmap-tc)# class type traffic-class cmap_tc
Switch(config-pmap-tc-c)# queue-limit dynamic 2
Related Commands

show qos interface egress

10.1.22 random-detect

Command Purpose

Use this command to configure random detect parameters.

Command Syntax

random-detect maximum-threshold MAX [ minimum-threshold MIN ] [ ecn ]

no random-detect

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAX</td>
<td>maximum value in buffer cell, 288 bytes per cell</td>
<td>range 32-1023.</td>
</tr>
<tr>
<td>MIN</td>
<td>minimum value in buffer cell, 288 bytes per cell. MIN default value is MAX / 8 if no set.</td>
<td>range 32-1023</td>
</tr>
<tr>
<td>ecn</td>
<td>enable ecn</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Config-pmap-c Configuration

Default

None

Usage

Queue-limit, queue-limit dynamic and random-detect are conflict.

Examples

Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
Switch(config-pmap-tc)# class type traffic-class cmap_tc
Switch(config-pmap-tc-c)# random-detect maximum-threshold 200 ecn

Related Commands

show qos interface egress

10.1.23 shape rate

Command Purpose

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

Command Syntax

shape rate RATE

no shape rate

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RATE</td>
<td>The value for commit information rate</td>
<td>range 0 - 100,000,000.</td>
</tr>
</tbody>
</table>

Command Mode

Config-pmap-c Configuration
**Default**

None

**Usage**

None

**Examples**

Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
Switch(config-pmap-tc)# class type traffic-class cmap_tc
Switch(config-pmap-tc-c)# shape rate 100000

**Related Commands**

show qos interface egress

**10.1.24 service-policy type qos**

**Command Purpose**

Use this command to apply a policy-map to an interface to affect the traffic classification rules. To remove the policy-map from the interface, use the no form of this command.

**Command Syntax**

service-policy type qos input NAME

no service-policy type qos input

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Policy-map name</td>
<td>The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

None

**Usage**

None

**Examples**

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# service-policy type qos input pmap_qos

**Related Commands**

policy-map type qos
10.1.25  service-policy type traffic-class

Command Purpose

Use this command to apply a policy-map to an interface to affect the traffic queuing rules. To remove the policy-map from the interface, use the no form of this command.

Command Syntax

service-policy type traffic-class NAME
no service-policy type traffic-class

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Policy-map name</td>
<td>The name can be a maximum of 40 characters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration
Configure-qos-global-view

Default

None

Usage

This command is used to apply queuing and priority-flow-control parameters on interface.

Examples

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# service-policy type traffic-class pmap_tc

Related Commands

policy-map type qos
class-map type traffic-class

10.1.26  qos shape rate

Command Purpose

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

Command Syntax

qos shape rate pir PIR (ecn-percentage PERCENTAGE | )
no qos shape rate
### Command Mode

Interface Configuration

### Default

None

### Usage

None

### Examples

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# qos shape rate 1000

### Related Commands

10.1.27 show class-map

### Command Purpose

Use this command to show class map information.

### Command Syntax

```
show class-map [NAME]
```

### Command Mode

Privileged EXEC

### Default

None

### Usage

None

### Examples

Switch# show class-map cos1
CLASS-MAP-NAME: cos1 (qos)
   match cos 1
Related Commands

class-map type qos

10.1.28  show policy-map

Command Purpose

Use this command to show policy map information.

Command Syntax

show policy-map [ NAME ]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Policy map's name</td>
<td>The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

Switch# show policy-map q1

POLICY-MAP-NAME: q1 (qos)
  State: attached

CLASS-MAP-NAME: cos0
  match cos 0
  set traffic-class 7
  statistics : enable
  policer color-aware cir 10000000 cbs 640000 ebs 640000 statistics

Related Commands

policy-map type qos

10.1.29  show qos aggregate-policer

Command Purpose

Use this command to show aggregator-policer information.

Command Syntax

show qos aggregate-policer NAME
NAME | aggregate policer name | The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

Switch# show qos aggregate-policer example

| Aggrate policer: test | color blind | CIR 1000 kbps, CBS 640000 bytes, EBS 640000 bytes | drop violate packets |

**Related Commands**

aggregate-policer

10.1.30 show qos interface ingress

**Command Purpose**

Use this command to show interface ingress information.

**Command Syntax**

show qos interface NAME ingress { cos-policy | inner-cos-policy | dscp-policy | acl-policy }

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>interface name</td>
<td>Support physical/aggregation/vlan ports</td>
</tr>
<tr>
<td>cos-policy</td>
<td>show cos mapping information</td>
<td>-</td>
</tr>
<tr>
<td>inner-cos-policy</td>
<td>show inner cos mapping information</td>
<td>-</td>
</tr>
<tr>
<td>dscp-policy</td>
<td>show dscp mapping information</td>
<td>-</td>
</tr>
<tr>
<td>acl-policy</td>
<td>show acl mapping information</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None
Usage

None

Examples

Switch# show qos interface eth-0-1 ingress cos-policy

<table>
<thead>
<tr>
<th>CoS</th>
<th>TC</th>
<th>Color</th>
<th>Mark-Type</th>
<th>Mark-Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>green</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>green</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>green</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>green</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>green</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>green</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>green</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>green</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Related Commands

service-policy type qos
service-policy type traffic-class

10.1.31 show qos interface egress

Command Purpose

Use this command to show interface egress information.

Command Syntax

show qos interface IFNAME egress

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>interface name</td>
<td>Support physical/aggregation/vlan ports</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

Switch# show qos interface eth-0-1 egress

<table>
<thead>
<tr>
<th>TC</th>
<th>Priority</th>
<th>Bandwidth</th>
<th>Shaping(kbps)</th>
<th>Drop-Mode</th>
<th>Queue-Limit(Max/Min)</th>
<th>ECN</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>Remaining</td>
<td>-</td>
<td>dynamic</td>
<td>level 0</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>dynamic</td>
<td>level 0</td>
<td>-</td>
</tr>
</tbody>
</table>
Related Commands

service-policy type qos

10.1.32  show qos aggregate-policer statistics

Command Purpose
Use this command to show aggregator-policer's statistics information.

Command Syntax

show qos aggregate-policer NAME statistics

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>aggregate policer name</td>
<td>The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

Switch# show qos aggregate-policer example statistics

Aggreate policer: example
rfc2697    bps  color-aware
CIR 1000000 kbps, CBS 640000 bytes, EBS 640000 bytes
Conform packets transmit
Exceed packets transmit
Violate packets drop
Statistics:
<table>
<thead>
<tr>
<th>Type</th>
<th>Packets</th>
<th>Bytes</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conform 0</td>
<td>0</td>
<td>0</td>
<td>Transmit</td>
</tr>
<tr>
<td>Exceed</td>
<td>0</td>
<td>0</td>
<td>Transmit</td>
</tr>
<tr>
<td>Violate 0</td>
<td>0</td>
<td>0</td>
<td>Drop</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
</tbody>
</table>

Related Commands

service-policy type traffic-class
10.1.33  show policy-map type qos statistics interface ace

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

Command Syntax
show policy-map type qos statistics interface NAME input ace (ace-based | class-based | ) ( class CMAP-NAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>interface name</td>
<td>-</td>
</tr>
<tr>
<td>input</td>
<td>The statistics of input direction will be shown</td>
<td>-</td>
</tr>
<tr>
<td>ace-based</td>
<td>The statistics of matching ace will be shown</td>
<td>-</td>
</tr>
<tr>
<td>class-based</td>
<td>statistics of class-map will be shown</td>
<td>-</td>
</tr>
<tr>
<td>CMAP-NAME</td>
<td>statistics of the specified class-map can be shown</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
Using this command, the flow policer stats can be shown when class-based is specified and flow policer stats is enabled.
The statistics of ace-based and class-based have results only when the statistics is enabled.

Examples
Switch# show policy-map type qos statistics interface eth-0-1 input ace class-based
  Interface: eth-0-1
  Input service policy type qos: q1
  Class name: cos0, operator: match-any(match 0 bytes 0)
  Class name: cos1, operator: match-any(match 0 bytes 0)

Switch# show policy-map type qos statistics interface eth-0-1 input ace ace-based
  Interface: eth-0-1
  Input service policy type qos: q1
  Class name: cos0, operator: match-any
    match cos 0 ( 0 match 0 bytes)
    total 0 match 0 bytes
  Class name: cos1, operator: match-any
    match cos 1 ( 0 match 0 bytes)
    total 0 match 0 bytes

Related Commands
10.1.34  show policy-map type qos statistics interface policer

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

Command Syntax
show policy-map type qos statistics interface IFNAME input policer ( class CMAP-NAME )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>interface name</td>
<td>Support physical/aggregation/vlan ports</td>
</tr>
<tr>
<td>input</td>
<td>The statistics of input direction will be shown</td>
<td>-</td>
</tr>
<tr>
<td>CMAP-NAME</td>
<td>statistics of the specified class-map can be shown</td>
<td>The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
The statistics have results only when the policer statistics is enabled.

Examples
Switch# show policy-map type qos statistics interface eth-0-1 input policer
Interface: eth-0-1
Input service policy type qos: q1
   Class name: cos0, operator : match-any
   Class name: cos1, operator : match-any
      Policer(mode rfc2697, rate mode bps, CIR 10000000 kbps, CBS 640000 bytes, EBS 640000 bytes, color mode color-aware, conform transmit, exceed transmit, violate drop)
         Conform packets 0, bytes 0
         Exceed packets 0, bytes 0
         Violate packets 0, bytes 0

Related Commands
service-policy type qos
service-policy type traffic-class

10.1.35  show qos interface statistics policer

Command Purpose
Use this command to display port statistics.

Command Syntax
show qos interface IFNAME statistics policer ( input | output )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical/aggregation/vlan ports</td>
</tr>
</tbody>
</table>
**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

Switch# show qos interface eth-0-1 statistics policer input

<table>
<thead>
<tr>
<th>Interface: eth-0-1</th>
<th>Input port policer: rfc2697 bps color-aware</th>
<th>CIR 2000000 kbps, CBS 640000 bytes, EBS 640000 bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Conform packets transmit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Exceed packets transmit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Violate packets drop</td>
<td></td>
</tr>
</tbody>
</table>

Statistics:

<table>
<thead>
<tr>
<th>Type</th>
<th>Packets</th>
<th>Bytes</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conform 0</td>
<td>0</td>
<td>0</td>
<td>Transmit</td>
</tr>
<tr>
<td>Exceed 0</td>
<td>0</td>
<td>0</td>
<td>Transmit</td>
</tr>
<tr>
<td>Violate 0</td>
<td>0</td>
<td>0</td>
<td>Drop</td>
</tr>
</tbody>
</table>

Total 0 0 -

**Related Commands**

service-policy type qos

**10.1.36 show qos interface statistics queue**

**Command Purpose**

Use this command to display the statistics of traffic class per interface.

**Command Syntax**

show qos interface IFNAME statistics queue

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical/aggregation/vlan ports</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

Switch# show qos interface eth-0-1 statistics queue

<table>
<thead>
<tr>
<th>Queue</th>
<th>Transmit-packets</th>
<th>Transmit-Bytes</th>
<th>Drop-packets</th>
<th>Drop-Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>UC0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>UC1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Related Commands

service-policy type traffic-class

10.1.37 clear qos aggregate-policer statistics

Command Purpose

Use this command to clear aggregate policing statistics.

Command Syntax

clear qos aggregate-policer NAME statistics

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Aggregate policer name.</td>
<td>The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

Switch# clear qos aggregate-policer example statistics

Related Commands

show qos aggregate-policer statistics

10.1.38 clear policy-map type qos statistics interface ace

Command Purpose

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

Command Syntax

clear policy-map type qos statistics interface IFNAME input ace
**Parameter** | **Parameter Description** | **Parameter Value**
--- | --- | ---
IFNAME | Interface name | Support physical/aggregation/vlan ports

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**

Switch# clear policy-map type qos statistics interface eth-0-1 input ace

**Related Commands**
show policy-map type qos statistics interface

**10.1.39 clear policy-map type qos statistics ace**

**Command Purpose**
Use this command to clear all the ace statistics of policy-map.

**Command Syntax**
show policy-map type qos statistics [ input ] ace

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>input</td>
<td>The statistics of input direction will be clear</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**

Switch# clear policy-map type qos statistics input ace

**Related Commands**
show policy-map type qos statistics ace
10.1.40 clear policy-map type qos statistics interface policer

Command Purpose
Use this command to clear the policer statistics of policy-map on interface.

Command Syntax
```
clear policy-map type qos statistics interface IFNAME input policer
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name.</td>
<td>Support physical/aggregation/vlan ports</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
```
Switch# clear policy-map type qos statistics interface eth-0-1 input policer
```

Related Commands
```
show policy-map type qos statistics interface policer
```

10.1.41 clear policy-map type qos statistics policer

Command Purpose
Use this command to clear all the policer statistics of policy-map.

Command Syntax
```
clear policy-map type qos statistics [ input ] policer
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>input</td>
<td>The statistics of input direction will be clear</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
```
Switch# clear policy-map type qos statistics input policer
```
Related Commands

show policy-map type qos statistics policer

10.1.42 clear qos interface statistics policer

Command Purpose

Use this command to clear port policer statistics.

Command Syntax

clear qos interface IFNAME statistics policer ( input | output )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name.</td>
<td>Support physical/aggregation/vlan ports</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

Switch# clear qos interface eth-0-1 statistics policer input

Related Commands

clear qos interface statistics policer

10.1.43 clear qos interface statistics queue

Command Purpose

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

Command Syntax

clear qos interface IFNAME statistics queue

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name.</td>
<td>Support physical/aggregation/vlan ports</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None
Examples
Switch# clear qos interface eth-0-1 statistics queue

Related Commands
show qos interface statistics queue

10.1.44 flow-policer number

Command Purpose
To set the number of policers for qos, such as normal and extend mode.

Command Syntax
Flow-policer number ( normal | extend )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>normal</td>
<td>Normal mode supports 576 policers</td>
<td>-</td>
</tr>
<tr>
<td>extend</td>
<td>Extend mode supports 3064 policers</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
Normal

Usage
When reset the number of policers, it needs to save the configuration and restart the switch.

Examples
Switch# configure terminal
Switch(config)# flow-policer number extend

% Configuration about flow-policer number has been stored, but cannot take effect until the next reload.
% When setting the extend number of policers, it only supports the 10G rate of policers, please check the rate of policers.

Related Commands
show policy-map type qos statistics interface ace
Chapter 11 Security Commands

11.1 Port Security Commands

11.1.1 switchport port-security

Command Purpose
To enable port security on an interface, use the switchport port-security command. To disable port security, use the no switchport port-security command.

Command Syntax
switchport port-security
no switchport port-security

Command Mode
Interface Configuration

Default
Disabled

Usage
When disable port-security, all the port-security mac address entries which are learnt dynamically will be cleared. The static port-security mac address will be ineffective but not be cleared.

Examples
This example shows how to enable port security on an interface:

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

This example shows how to disable port security on an interface:

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

Related Commands
show port-security interface

11.1.2 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC_ADDR</td>
<td>Static port-security mac address</td>
<td>MAC address in HHHH.HHHH.HHHH format</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>Static port-security VLAN id</td>
<td>1-4094</td>
</tr>
</tbody>
</table>
**Command Mode**

Interface Configuration

**Default**

None

**Usage**

None

**Examples**

This example shows how to configure static port-security mac address:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport port-security mac-address 0.0.1 vlan 1
```

This example shows how to delete static port-security mac address:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport port-security mac-address 0.0.1 vlan 1
```

**Related Commands**

show mac address-table

### 11.1.3 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAXIMUM</td>
<td>Maximum number of secure MAC addresses for the interface</td>
<td>0-16384</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

1

**Usage**

If the new maximum is smaller than the current secure addresses on the interface, the configuration is rejected.

Once the secure MAC address number on the port reached the maximum number, no more address can be learnt on that port.

The maximum number 0 indicates that no dynamic secure MAC is allowed, only static secure MAC is supported.
Examples

This example sets the maximum number of secure MAC addresses on a port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport port-security maximum 1024
```

This example restores the maximum number of secure MAC addresses on a port to default value:

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

Related Commands

- `switchport port-security violation`
- `show port-security maximum mac-num interface IFNAME`

### 11.1.4 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>protect</td>
<td>Discard packet silently</td>
<td>-</td>
</tr>
<tr>
<td>restrict</td>
<td>Discard packet and print log</td>
<td>-</td>
</tr>
<tr>
<td>errdisable</td>
<td>Discard packet, log and set the interface error-disabled</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

Discard packet silently

**Usage**

To use this command, enable switchport port-security first

**Examples**

This example sets port-security violation to discard packets silently:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switch port-security violation protect
```

Related Commands

- `switchport port-security`
11.1.5 show port-security address-table

**Command Purpose**
Use this command to show port-security mac address-table.

**Command Syntax**

```
show port-security address-table [ dynamic | static ] [ interface IFNAME | vlan VLAN_ID | address MAC_ADDR ]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dynamic</td>
<td>Show the dynamically learnt entries</td>
<td>-</td>
</tr>
<tr>
<td>static</td>
<td>Show the statically configured entries</td>
<td>-</td>
</tr>
<tr>
<td>MAC_ADDR</td>
<td>Show the entries with specified mac address</td>
<td>MAC address in HHHH.HHHH.HHHH format</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Show the entries with specified interface name</td>
<td>Support physical ports</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>Show the entries with specified VLAN id</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**

This example shows port-security mac address-table on the Switch:

```
Switch# show port-security address-table
Secure Mac Address Table
---------------------------------------
Vlan | Mac Address | Type           | Ports |
-----|-------------|----------------|-------|
 1   | 0001.00ce.ef01 | SecureConfigured | eth-0-11 |
 41  | 001a.a02c.a1dc | SecureConfigured | eth-0-41 |
```

**Related Commands**
None

11.1.6 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Show the entries with specified interface name</td>
<td>Support physical ports</td>
</tr>
</tbody>
</table>
11.7 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Show the entries with specified interface name</td>
<td>Support physical ports</td>
</tr>
</tbody>
</table>

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
11.1.8 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Show the entries with specified</td>
<td>Support physical ports</td>
</tr>
<tr>
<td></td>
<td>interface name</td>
<td></td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows the port-security maximum mac-num on interface eth-0-1:

Switch# show port-security maximum mac-num interface eth-0-1
Maximum dynamic MAC addresses : 1

Related Commands
switchport port-security maximum
show port-security current mac-num interface

11.2 Vlan Security Commands

11.2.1 vlan mac-limit maximum

Command Purpose
Use this command to set maximum of mac addresses in specified vlan. Use the no vlan mac-limit maximum command to restore the default setting.

Command Syntax
vlan VLAN_ID mac-limit maximum MAXIMUM
no vlan VLAN_ID mac-limit maximum
### Parameter Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>VLAN id</td>
<td>1-4094</td>
</tr>
<tr>
<td>MAXIMUM</td>
<td>maximum of mac addresses</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

### Command Mode
VLAN Configuration

### Default
No mac-limit on all vlans

### Usage
The vlan must be created before this command

### Examples
This example shows how to set/unset maximum of mac addresses for specified vlan:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# vlan 2 mac-limit maximum 1000
Switch(config-vlan)# no vlan 2 mac-limit maximum
```

### Related Commands
show vlan-security

#### 11.2.2 vlan mac-limit action

### Command Purpose
Use this command to set action for specified vlan.
Use the no vlan mac-limit action command to restore the default setting.

### Command Syntax
`vlan VLAN_ID mac-limit action (discard | warn | forward)`

```plaintext
no vlan VLAN_ID mac-limit action
```

### Parameter Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>VLAN id</td>
<td>1-4094</td>
</tr>
<tr>
<td>discard</td>
<td>the count of mac addresses reaches the maximum, packets with unknown source mac address from this VLAN will be discarded</td>
<td>-</td>
</tr>
<tr>
<td>warn</td>
<td>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</td>
<td>-</td>
</tr>
<tr>
<td>forward</td>
<td>if the count of mac addresses reaches the maximum, all packets from this VLAN will be forwarded without neither mac learning nor warning log</td>
<td>-</td>
</tr>
</tbody>
</table>

### Command Mode
VLAN Configuration
Default
Forward

Usage
The vlan must be created before this command.

Examples
This example shows how to set/unset action for specified vlan:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# vlan 2 mac-limit action warn
Switch(config-vlan)# no vlan 2 mac-limit action
```

Related Commands
show vlan-security

11.2.3 vlan mac learning

Command Purpose
Use this command to enable/disable mac learning for specified vlan.

Command Syntax
```
vlan VLAN_ID mac learning ( enable | disable )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>VLAN id</td>
<td>1-4094</td>
</tr>
<tr>
<td>enable</td>
<td>Enable learning</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>Disable learning</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
VLAN Configuration

Default
Enable

Usage
The vlan must be created before using this command.

Examples
This example shows how to enable mac learning for specified vlan:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# vlan 2 mac learning enable
```

Related Commands
show vlan-security
11.2.4 show vlan-security

Command Purpose
Use this command to show configuration about vlan security.

Command Syntax
show vlan-security (vlan VLAN_ID)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>VLAN id</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to show configuration about vlan security:

Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# vlan 2 mac-limit maximum 1000
Switch(config-vlan)# vlan 2 mac-limit action warn
Switch# show vlan-security
Vlan learning-en max-mac-count cur-mac-count action
-----------------------------------------------------------------------------------
2 Enable 1000 0 Warn

Related Commands
vlan mac-limit maximum
vlan mac-limit action

11.3 Time Range Commands

11.3.1 periodic

Command Purpose
Use this command to define the periodic time and date in time range.

Command Syntax
periodic HH:MM WEEKDAY to HH:MM ( WEEKDAY | )
periodic HH:MM ( weekdays | weekend | daily ) to HH:MM
Parameter | Parameter Description | Parameter Value
--- | --- | ---
**HH:MM** | Starting time or Ending time | Hour, minute in HH:MM Format HH is 0-23
**weekdays** | Monday thru Friday | -
**weekend** | Saturday and Sunday | -
**daily** | Every day of the week | -
**WEEKDAY** | Day of the week (First three letters of the weekday) | A case insensitive string of Monday - Sunday, at least 3 characters when using abbreviation.

**Command Mode**

Time Range Configuration

**Default**

None

**Usage**

Comparing with the absolute time, choose an appropriate type.

**Examples**

This example shows how to define a time range started from 00:00 Monday and ended by 18:00 Wednesday in weekly period:

Switch# configure terminal
Switch(config)# time-range my-time-range
Switch(config-tm-range)# periodic 00:00 mon to 18:00 wed

This example shows how to define a time range started from 09:00 and ended by 17:00 every day:

Switch# configure terminal
Switch(config)# time-range my-time-range
Switch(config-tm-range)# periodic 09:00 daily to 17:00

**Related Commands**

absolute

11.3.2 show time-range

**Command Purpose**

Use this command to show the information of time-range.

**Command Syntax**

show time-range ( **TIME-RANGE-NAME** | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TIME-RANGE-NAME</strong></td>
<td>the name of the time range. Show all the time ranges when the name is not specified</td>
<td>String with up to 40 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC
Default
None

Usage
If no time range is specified, all time-ranges in the system should be shown.

Examples
This example shows how to display the information of all the time ranges:

Switch# show time-range
  time-range range1
  periodic 00:01 weekdays to 12:01

Related Commands
time-range

11.4 ACL Commands

11.4.1 mac access-list

Command Purpose
Use this command to create MAC ACL and then enter MAC ACL in global configuration mode. Use no mac access-list command to delete the MAC ACL.

Command Syntax
mac access-list ACL_NAME
no mac access-list ACL_NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL_NAME</td>
<td>The name of the MAC ACL</td>
<td>A string with up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
If the system already has a MAC ACL with the same name, this command will enter the MAC ACL configuration mode. However, if the ACL name is used by other type of ACL, a prompt message will be shown.

When the name is not used by any ACL, this command is to create the MAC ACL firstly and then enter the MAC ACL configuration mode.

Examples
This example shows how to create a MAC ACL named list_mac_1 and then enter the MAC ACL configuration mode:

Switch# configure terminal
Switch(config)# mac access-list list_mac_1
Switch(config-mac-acl)#

This example shows how to remove the MAC ACL named list_mac_1:

Switch# configure terminal
Switch(config)# no mac access-list list_mac_1
Related Commands

match access-group

11.4.2 sequence-num

Command Purpose

Use this command to remove a filter from MAC ACL.

Command Syntax

no sequence-num SEQUENCE_NUM

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of a IP/MAC filter</td>
<td>1-131071</td>
</tr>
</tbody>
</table>

Command Mode

MAC ACL Configuration

IP ACL Configuration

Default

None

Usage

User can delete a ACL which is already attached to the class-map and used by a interface immediately.

Examples

This example shows how to remove a filter with the sequence-num 10 from MAC ACL:

Switch# configure terminal
Switch(config)# mac access-list list_mac_1
Switch(config-mac-acl)# no sequence-num 10

This example shows how to remove a filter with the sequence-num 10 from IP ACL:

Switch# configure terminal
Switch(config)# ip access-list list_ip_1
Switch(config-ip-acl)# no sequence-num 10

Related Commands

deny
deny tcp
deny udp
deny icmp
deny igmp
permit
permit tcp
permit udp
permit icmp
permit igmp
### 11.4.3 deny src-mac

**Command Purpose**

Use this command to create a MAC filter for discarding ongoing packets matching the filter rule.

**Command Syntax**

\[
( \text{SEQUENCE\_NUM} \mid \) \text{deny src-mac} \left( \text{any} \mid \text{MAC\_ADDR} \mid \text{MAC\_ADDR\_MASK} \mid \text{host} \mid \text{MAC\_ADDR} \right) \left( \text{dest-mac} \left( \text{any} \mid \text{MAC\_ADDR} \mid \text{MAC\_ADDR\_MASK} \mid \text{host} \mid \text{MAC\_ADDR} \right) \right) \left( \text{untag-vlan} \left( \text{VLAN\_ID} \mid \text{cos} \mid \text{INNER\_VLAN} \mid \text{INNER\_COS} \right) \right) \left( \text{protocol} \left( \text{arp} \mid \text{rarp} \mid \text{ETH\_TYPE} \right) \right) \left( \text{packet-length} \text{OPERATOR} \text{LENGTH} \right) \left( \text{TIME\_RANGE\_NAME} \right) \]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>any</td>
<td>Any host</td>
<td>-</td>
</tr>
<tr>
<td>MAC_ADDR</td>
<td>The MAC address and its wildcard bits</td>
<td>MAC and wildcard in HHHH.HHHH.HHHH format</td>
</tr>
<tr>
<td>host MAC_ADDR</td>
<td>The host with a specified MAC address</td>
<td>MAC address in HHHH.HHHH.HHHH format</td>
</tr>
<tr>
<td>dest-mac</td>
<td>Destination MAC address</td>
<td>-</td>
</tr>
<tr>
<td>untag-vlan</td>
<td>Without vlan tag</td>
<td>-</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>VLAN-ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>cos</td>
<td>CoS Value</td>
<td>0-7</td>
</tr>
<tr>
<td>INNER_VLAN</td>
<td>Inner VLAN-ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>INNER_COS</td>
<td>Inner CoS value</td>
<td>0-7</td>
</tr>
<tr>
<td>protocol</td>
<td>The protocol type which including ARP, RARP or Ether type</td>
<td>-</td>
</tr>
<tr>
<td>arp</td>
<td>ARP protocol</td>
<td>-</td>
</tr>
<tr>
<td>arp-op-code</td>
<td>arp-op-code</td>
<td>0-65535</td>
</tr>
<tr>
<td>rarp</td>
<td>RARP protocol</td>
<td>-</td>
</tr>
<tr>
<td>ETH_TYPE</td>
<td>Ether type</td>
<td>0-0xFFFF</td>
</tr>
<tr>
<td>TIME_RANGE_NAME</td>
<td>The time-range used by the MAC filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**Command Mode**

MAC ACL Configuration

**Default**

None
Usage

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the MAC ACL. i.e. when the maximum existing sequence number is 100, the sequence number of subsequent created MAC filter is 110. Eth-type is not supported in egress ACL.

Examples

This example shows how to create a filter in MAC ACL to deny the packets with source MAC address 001A.A02C.A1DF:

Switch# configure terminal
Switch(config)# mac access-list list_mac_1
Switch(config-mac-acl)# 1 deny src-mac host 001A.A02C.A1DF

This example shows how to create a filter in MAC ACL to deny all the packets:

Switch# configure terminal
Switch(config)# mac access-list list_mac_1
Switch(config-mac-acl)# 2 deny src-mac any

This example shows how to create a filter in MAC ACL to deny the packet whose source MAC address is between the ranges specified:

Switch# configure terminal
Switch(config)# mac access-list list_mac_1
Switch(config-mac-acl)# 3 deny src-mac 001A.A02C.A1DF 001A.A02C.0000

Related Commands

no sequence-num

11.4.4 permit src-mac

Command Purpose

Use this command to create a MAC filter for allowing packets matching the filter rule to be delivered.

Command Syntax

```plaintext
(SEQUENCE_NUM | ) permit src-mac ( any | MAC_ADDR MAC_ADDR_MASK | host MAC_ADDR ) ( dest-mac ( any | MAC_ADDR MAC_ADDR_MASK ) ) ( untranslated ) ( VLAN ( | ) ( cos COS ) ( inner-vlan INNER_VLAN ) ) ( inner-cos INNER_COS ) ( protocol ( arp ( | ) | ) | ) | ) ( packet-length OPERATOR LENGTH ) | ) ) ( TIME_RANGE_NAME )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>any</td>
<td>Any host</td>
<td>-</td>
</tr>
<tr>
<td>MAC_ADDR MAC_ADDR_MASK</td>
<td>The MAC address and its wildcard bits. MAC and wildcard in HHHH.HHHH.HHHH format</td>
<td></td>
</tr>
<tr>
<td>host MAC_ADDR</td>
<td>The host with a specified MAC address. MAC address in HHHH.HHHH.HHHH format</td>
<td></td>
</tr>
<tr>
<td>dest-mac</td>
<td>Destination MAC address</td>
<td>-</td>
</tr>
<tr>
<td>untranslated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN-ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>inner-vlan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INNER_VLAN</td>
<td>Inner VLAN-ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>cos</td>
<td>CoS</td>
<td>0-7</td>
</tr>
<tr>
<td>inner-cos</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Parameter Description</td>
<td>Parameter Value</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>INNER_COS</td>
<td>Inner CoS</td>
<td>0-7</td>
</tr>
<tr>
<td>protocol</td>
<td>The protocol type which including ARP, RARP or Ether type</td>
<td>-</td>
</tr>
<tr>
<td>arp</td>
<td>ARP protocol</td>
<td>-</td>
</tr>
<tr>
<td>arp-op-code</td>
<td>arp op code</td>
<td>0-65535</td>
</tr>
<tr>
<td>rarp</td>
<td>RARP protocol</td>
<td>-</td>
</tr>
<tr>
<td>ETH_TYPE</td>
<td>Ether type</td>
<td>0-0xFFFF</td>
</tr>
<tr>
<td>TIME_RANGE_NAME</td>
<td>Specify the name of time-range used by the MAC filter</td>
<td>String with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**Command Mode**

MAC ACL Configuration

**Default**

None

**Usage**

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the MAC ACL. i.e. when the maximum existing sequence number is 105, the sequence number of subsequent created MAC filter is 115. Eth-type is not supported in egress ACL.

**Examples**

This example shows how to create a filter in MAC ACL to permit the packets with source MAC address 001A.A02C.A1DF:

```
Switch# configure terminal
Switch(config)# mac access-list list_mac_1
Switch(config-mac-acl)# 1 permit src-mac host 001A.A02C.A1DF
```

This example shows how to create a filter in MAC ACL to permit all the packets:

```
Switch# configure terminal
Switch(config)# mac access-list list_mac_1
Switch(config-mac-acl)# 2 permit src-mac any
```

This example shows how to create a filter in MAC ACL to permit the packets with source MAC address between the ranges specified:

```
Switch# configure terminal
Switch(config)# mac access-list list_mac_1
Switch(config-mac-acl)# 3 permit src-mac 001A.A02C.A1DF 001A.A02C.0000
```

**Related Commands**

no sequence-num

11.4.5 remark

**Command Purpose**

Use this command to add remarks for the MAC ACL.

To remove remarks of the MAC ACL, use the no form of this command.
Command Syntax
remark REMARK
no remark

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>REMARK</td>
<td>The remarks of the MAC ACL</td>
<td>String with up to 100 characters</td>
</tr>
</tbody>
</table>

Command Mode
MAC ACL Configuration
IP ACL Configuration

Default
None

Usage
The remarks are up to 100 characters. The exceed parts will not be stored and will be truncated.

Examples
This example shows how to add a remark to describe the MAC ACL:

Switch# configure terminal
Switch(config)# mac access-list list_mac_1
Switch(config-mac-acl)# remark remark of List for mac

This example shows how to remove the remark of the MAC ACL:

Switch# configure terminal
Switch(config)# mac access-list list_mac_1
Switch(config-mac-acl)# no remark

Related Commands
mac access-list

11.4.6 show access-list mac

Command Purpose
Use this command to show the MAC ACL information.

Command Syntax
show access-list mac (ACL_NAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL_NAME</td>
<td>The name of the MAC ACL</td>
<td>String with up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
If no mac acl are specified, all mac access-lists in the system should be shown.
Examples

This example shows how to show the MAC ACL information:

```
Switch# show access-list mac

mac access-list list_mac_1
  10 deny src-mac host 0000.0001.0002
  20 permit src-mac any
```

Related Commands

mac access-list

11.4.7 ip access-list

Command Purpose

Use this command to create IP ACL and then enter IP ACL configuration mode.
To remove this ACL, use the no form of this command.

Command Syntax

```
ip access-list ACL_NAME
no ip access-list ACL_NAME
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL_NAME</td>
<td>The name of an IP ACL</td>
<td>String with up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

If the system already has an IP ACL with the same name, this command will enter the IP ACL configuration mode. However, if the ACL name is used by other type of ACL, a prompt message will be shown.
When the name is not used by any ACL, this command is to create the IP ACL firstly and then enter the IP ACL configuration mode.

Examples

This example shows how to create an IP ACL named list_ipv4_1 and then enter the IP ACL configuration mode:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)#
```

This example shows how to remove the IP ACL named list_ipv4_1:

```
Switch# configure terminal
Switch(config)# no ip access-list list_ipv4_1
```

Related Commands

match access-group
11.4.8 deny

Command Purpose
Use this command to discard ongoing IP packets matching the IP filter.

Command Syntax

```
( SEQUENCE_NUM | deny ( PROTO_NUM | any ) ( SRC_MAC SRC_MAC_MASK | any | host SRC_MAC | ( DST_MAC DST_MAC_MASK | any | host DST_MAC ) ( ip-precedence PRECEDENCE | dscp DSCP ) | ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet ) ) ( options ) ( packet-length OPERATOR LENGTH ) ) ( TIME_RANGE_NAME )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of the filter in IP ACL.</td>
<td>1-131071</td>
</tr>
<tr>
<td></td>
<td>An auto-generated sequence number will be assigned to the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>filter if this field is not presented.</td>
<td></td>
</tr>
<tr>
<td>PROTO_NUM</td>
<td>An IP protocol number</td>
<td>0-255</td>
</tr>
<tr>
<td>any</td>
<td>Any IP protocol</td>
<td>-</td>
</tr>
<tr>
<td>SRC_MAC SRC_MAC_MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>host SRC_MAC</td>
<td>The source IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>DST_MAC DST_MAC_MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>host DST_MAC</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td>-</td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td>-</td>
</tr>
<tr>
<td>TIME_RANGE_NAME</td>
<td>The time-range used by the filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

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, 10.10.0.0.0.0.255 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
do sequence-num

11.4.9 deny tcp

Command Purpose
Use this command to reject TCP packets matching the IP filter.

Command Syntax
```
( SEQUENCE_NUM | ) deny tcp ( SRC_MAC SRC_MAC_MASK | any | host SRC_MAC ) ( src-port OPERATOR SRC_PORT | ) ( DST_MAC DST_MAC_MASK | any | host DST_MAC ) ( dst-port OPERATOR DST_PORT | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( established | ( match-any | match-all FLAG-NAME | ) | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment | routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( TIME_RANGE_NAME )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_MAC SRC_MAC_MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>any</td>
<td>Any source host</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_MAC</td>
<td>The source IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>OPERATOR SRC_PORT</td>
<td>Source port operator and value</td>
<td>Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>DST_MAC DST_MAC_MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>host DST_MAC</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>Parameter</td>
<td>Parameter Description</td>
<td>Parameter Value</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>OPERATOR DST_PORT</td>
<td>Destination port operator and value</td>
<td>Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>established</td>
<td>Match established connections</td>
<td>-</td>
</tr>
<tr>
<td>match-any</td>
<td>Match any of the flag-name</td>
<td>-</td>
</tr>
<tr>
<td>FLAG-NAME</td>
<td>Match all the flag-name, including ack, fin, psh, rst, syn and urg</td>
<td>ack, fin, psh, rst, syn and urg</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td>-</td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td>-</td>
</tr>
<tr>
<td>TIME_RANGE_NAME</td>
<td>The time-range used by the IP filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**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
```

This example shows how to create a filter in IP ACL to deny the TCP packets with the source IP address 1.1.1.1, source port 0-100:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 2 deny tcp host 1.1.1.1 src-port range 0 100 any
```

This example shows how to create a filter in IP ACL to deny any TCP packets in established TCP streams:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 3 deny tcp any any established
```

This example shows how to create a filter in IP ACL to deny the TCP ACK packets with the source IP address 1.1.1.1:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 4 deny tcp 10.10.10.0 0.0.0.0 any match-any ack
```

Related Commands

no sequence-num

11.4.10 deny udp

Command Purpose

Use this command to reject UDP packets matching the IP filter.

Command Syntax

```
(SEQUENCE_NUM | ) deny udp ( SRC_MAC SRC_MAC_MASK | any | host SRC_MAC ) ( src-port OPERATOR SRC_PORT | ) ( DST_MAC DST_MAC_MASK | any | host DST_MAC ) ( dst-port OPERATOR DST_PORT | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( TIME_RANGE_NAME | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_MAC SRC_MAC_MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>any</td>
<td>Any source host</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_MAC</td>
<td>The source IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>OPERATOR SRC_PORT</td>
<td>Source port operator and value</td>
<td>Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>DST_MAC DST_MAC_MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>Parameter</td>
<td>Parameter Description</td>
<td>Parameter Value</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>host DST_MAC</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>OPERATOR DST_PORT</td>
<td>Destination port operator and value</td>
<td>Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td>-</td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td>-</td>
</tr>
<tr>
<td>TIME_RANGE_NAME</td>
<td>The time-range used by the IP filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**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)# access-list 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-ac)# 2 deny udp host 1.1.1.1 src-port eq 10 any dst-port lt 2000

Related Commands

no sequence-num

11.4.11 deny icmp

Command Purpose

Use this command to reject ICMP packets matching the IP filter.

Command Syntax

( SEQUENCE_NUM | ) deny icmp ( SRC_MAC SRC_MAC MASK | any | host SRC_MAC ) ( DST_MAC DST_MAC MASK | any | host DST_MAC )
( icmp-type TYPE-NUM ( icmp-code CODE-NUM | ) | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | )
( TIME_RANGE_NAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TYPE-NUM</td>
<td>ICMP message type</td>
<td>0-255</td>
</tr>
<tr>
<td>CODE-NUM</td>
<td>ICMP message code</td>
<td>0-255</td>
</tr>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of the filter in IP ACL. An auto-generated sequence number</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_MAC SRC_MAC MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>any</td>
<td>Any source host</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_MAC</td>
<td>The source IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>DST_MAC DST_MAC MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>host DST_MAC</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td>-</td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td>-</td>
</tr>
<tr>
<td>TIME_RANGE_NAME</td>
<td>The time-range used by the IP filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>
**Command Mode**

**IP ACL Configuration**

**Default**

None

**Usage**

This type of filter is mostly used to reject ICMP packets.

**Examples**

This example shows how to create a filter in IP ACL to deny any ICMP packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 1 deny icmp any any
```

This example shows how to create a filter in IP ACL to deny the ICMP packets with the icmp-type 3 and icmp-code 3:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 2 deny icmp any any icmp-type 3 icmp-code 3
```

**Related Commands**

no sequence-num

**11.4.12 deny igmp**

**Command Purpose**

Use this command to reject IGMP packets matching the IP filter.

**Command Syntax**

```
(SEQUENCE_NUM | ) deny igmp (SRC_MAC SRC_MAC_MASK | any | host SRC_MAC) (DST_MAC DST_MAC_MASK | any | host DST_MAC) (IGMP-TYPE | ) (ip-precedence PRECEDENCE | dscp DSCP | ) (non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment) (routed-packet | ) (options | ) (packet-length OPERATOR LENGTH | ) (TIME_RANGE_NAME | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP-TYPE</td>
<td>IGMP type</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>including dvmrp, host-query, host-report, mtrace, mtrace-response, precedence, trace, v2-leave, v2-report, v3-report</td>
</tr>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_MAC SRC_MAC_MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>any</td>
<td>Any source host</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_MAC</td>
<td>The source IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>Parameter</td>
<td>Parameter Description</td>
<td>Parameter Value</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>DST_MAC DST_MAC_MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>host DST_MAC</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td>-</td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td>-</td>
</tr>
<tr>
<td>TIME_RANGE_NAME</td>
<td>The time-range used by the IP filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**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:

```plaintext
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 1 deny igmp 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-ac)# 2 deny igmp host 1.1.1.1 any pim

Related Commands
no sequence-num
11.4.13 deny gre

Command Purpose
Use this command to reject GRE packets matching the IP filter.

Command Syntax
(SEQUENCE NUM | ) deny gre ( SRC MAC SRC MAC MASK | any | host SRC MAC ) ( DST MAC DST MAC MASK | any | host DST MAC ) ( key KEY mask KEY-MASK ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | ) ( options | ( packet-length OPERATOR LENGTH | ) ( TIME RANGE_NAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEY</td>
<td>GRE key</td>
<td>0-294967295</td>
</tr>
<tr>
<td>KEY-MASK</td>
<td>GRE key mask</td>
<td>0-0xffffffff</td>
</tr>
<tr>
<td>SEQUENCE NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC MAC SRC MAC MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>any</td>
<td>Any source host</td>
<td>-</td>
</tr>
<tr>
<td>host SRC MAC</td>
<td>The source IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>DST MAC DST MAC MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>host DST MAC</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td>-</td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td>-</td>
</tr>
</tbody>
</table>
### Command Mode

**IP ACL Configuration**

#### Default

None

#### Usage

This type of filter is mostly used to reject GRE packets.

Please reference to command “deny” for the other parameters.

#### Examples

This example shows how to create a filter in IP ACL to deny any GRE packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 1 deny gre any any key 0 mask 0
```

This example shows how to create a filter in IP ACL to deny the GRE packets with the source IP address 1.1.1.1, any destination IP address and the gre key is 10:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 2 deny gre host 1.1.1.1 any key 10 mask 0xffffffff
```

#### Related Commands

- no sequence-num

### 11.4.14 deny nvgre

#### Command Purpose

Use this command to reject NVGRE packets matching the IP filter.

#### Command Syntax

```
(SEQUENCE_NUM | ) deny nvgre ( SRC_MAC SRC_MAC_MASK | any | host SRC_MAC ) ( DST_MAC DST_MAC_MASK | any | host DST_MAC )
( vsid VSID_MASK | ) ( 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.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSID</td>
<td>NVGRE vsid</td>
<td>0-16777215</td>
</tr>
<tr>
<td>VSID-MASK</td>
<td>NVGRE vsid mask</td>
<td>0-0xFFFFFFFF</td>
</tr>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>PROTO_NUM</td>
<td>An IP protocol number</td>
<td>0-255</td>
</tr>
<tr>
<td>any</td>
<td>Any IP protocol</td>
<td>-</td>
</tr>
<tr>
<td>SRC_MAC SRC_MAC_MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>host SRC_MAC</td>
<td>The source IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>DST_MAC DST_MAC_MASK</td>
<td>destination IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>host DST_MAC</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td>-</td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td>-</td>
</tr>
<tr>
<td>TIME_RANGE_NAME</td>
<td>The time-range used by the IP filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**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 0xffffffff
```

**Related Commands**
no sequence-num

---

11.4.15 **permit**

**Command Purpose**
Use this command to permit packets matching the IP filter.

**Command Syntax**
```
(SEQUENCE_NUM | ) permit ( PROTO_NUM | any ) ( SRC_MAC SRC_MAC_MASK | any | host SRC_MAC | DST_MAC DST_MAC_MASK | any | host DST_MAC ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( TIME_RANGE_NAME | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>PROTO_NUM</td>
<td>An IP protocol number</td>
<td>0-255</td>
</tr>
<tr>
<td>any</td>
<td>Any IP protocol</td>
<td>-</td>
</tr>
<tr>
<td>SRC_MAC SRC_MAC_MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>host SRC_MAC</td>
<td>The source IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>DST_MAC DST_MAC_MASK</td>
<td>destination IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>host DST_MAC</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
</tbody>
</table>
### 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 0xffffffff
```

### Related Commands

- no sequence-num
- **11.4.16 permit tcp**

### Command Purpose

Use this command to permit TCP packets matching the IP filter.

### Table: DSCP Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
</tbody>
</table>

### Table: non-fragment Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td>-</td>
</tr>
</tbody>
</table>

### Table: first-fragment Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td>-</td>
</tr>
</tbody>
</table>

### Table: non-or-first-fragment Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
</tbody>
</table>

### Table: small-fragment Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td>-</td>
</tr>
</tbody>
</table>

### Table: non-first-fragment Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
</tbody>
</table>

### Table: routed-packet Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
</tbody>
</table>

### Table: options Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td>-</td>
</tr>
</tbody>
</table>

### Table: TIME RANGE NAME Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIME_RANGE_NAME</td>
<td>The time-range used by the IP filter</td>
<td>A string with up to 40 characters</td>
</tr>
</tbody>
</table>

### Table: OPERATOR Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
</tbody>
</table>

### Table: LENGTH Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>
## 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 | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_MAC SRC_MAC_MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>any</td>
<td>Any source host</td>
<td></td>
</tr>
<tr>
<td>host SRC_MAC</td>
<td>The source IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>OPERATOR SRC_PORT</td>
<td>Source port operator and value</td>
<td></td>
</tr>
<tr>
<td>DST_MAC DST_MAC_MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>host DST_MAC</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>OPERATOR DST_PORT</td>
<td>Destination port operator and value</td>
<td></td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>established</td>
<td>Match established connections</td>
<td></td>
</tr>
<tr>
<td>match-any</td>
<td>Match any of the flag-name</td>
<td></td>
</tr>
<tr>
<td>FLAG-NAME</td>
<td>Match all the flag-name, including ack, fin, psh, rst, syn and urg</td>
<td>ack, fin, psh, rst, syn and urg</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td></td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td></td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td></td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td></td>
</tr>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td></td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td></td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td></td>
</tr>
<tr>
<td>TIME_RANGE_NAME</td>
<td>The time-range used by the IP filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR LENGTH</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>
**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
```

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 routed-packet
```

This example shows how to create a filter in IP ACL to permit the TCP ACK packets with the source IP address 10.10.10.0:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 4 permit tcp 10.10.10.0 0.0.0.0 any match-any ack
```

**Related Commands**

no sequence-num

---

**11.4.17 permit udp**

**Command Purpose**

Use this command to permit UDP packets when the packets match this access-list.

**Command Syntax**

```
(SEQUENCE_NUM | ) permit udp ( SRC_MAC SRC_MAC_MASK | any | host SRC_MAC ) ( src-port OPERATOR SRC_PORT | ) ( DST_MAC DST_MAC_MASK | any | host DST_MAC ) ( dst-port OPERATOR DST_PORT | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH| ) ( TIME_RANGE_NAME | )
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_MAC SRC_MAC_MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>any</td>
<td>Any source host</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_MAC</td>
<td>The source IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>OPERATOR SRC_PORT</td>
<td>Source port operator and value</td>
<td>Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>DST_MAC DST_MAC_MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>host DST_MAC</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>OPERATOR DST_PORT</td>
<td>Destination port operator and value</td>
<td>Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td>-</td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td>-</td>
</tr>
<tr>
<td>TIME_RANGE_NAME</td>
<td>The time-range used by the IP filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**Command Mode**

IP ACL Configuration

**Default**

None
Usage

The fragments will be invalid when the layer 4 information is specified (i.e. src-port).

Examples

This example shows how to create a filter in IP ACL to deny any UDP packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 1 permit udp any any
```

This example shows how to create a filter in IP ACL to deny the UDP packets with the source IP address 1.1.1.1, source port 10, and destination port less than 2000:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 2 permit udp host 1.1.1.1 src-port eq 10 any dst-port lt 2000
```

Related Commands

no sequence-num

11.4.18 permit icmp

Command Purpose

Use this command to permit ICMP packets matching the IP filter.

Command Syntax

```
( SEQUENCE_NUM | ) permit icmp ( SRC_MAC SRC_MAC_MASK | any | host SRC_MAC ) ( DST_MAC DST_MAC_MASK | any | host DST_MAC )
( icmp-type TYPE-NUM ( icmp-code CODE-NUM | ) ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( TIME_RANGE_NAME | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp-type TYPE-NUM</td>
<td>ICMP message type</td>
<td>0-255</td>
</tr>
<tr>
<td>icmp-code CODE-NUM</td>
<td>ICMP message code</td>
<td>0-255</td>
</tr>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_MAC SRC_MAC_MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>any</td>
<td>Any source host</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_MAC</td>
<td>The source IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>DST_MAC DST_MAC_MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>host DST_MAC</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td>-</td>
</tr>
<tr>
<td>Parameter</td>
<td>Parameter Description</td>
<td>Parameter Value</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td>-</td>
</tr>
<tr>
<td>TIME_RANGE_NAME</td>
<td>The time-range used by the IP filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**Command Mode**

IP ACL Configuration

**Default**

None

**Usage**

This type of filter is mostly used to permit ICMP packets.

**Examples**

This example shows how to create a filter in IP ACL to permit any ICMP packets:

Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 1 permit icmp any any

This example shows how to create a filter in IP ACL to permit the ICMP packets with the icmp-type 3 and icmp-code 3:

Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 2 permit icmp any any icmp-type 3 icmp-code 3

**Related Commands**

deny icmp

no sequence-num

11.4.19 permit igmp

**Command Purpose**

Use this command to permit IGMP packets matching the IP filter.
### Command Syntax

(SEQUENCE_NUM | ) permit igmp (SRC_MAC SRC_MAC_MASK | any | host SRC_MAC) (DST_MAC DST_MAC_MASK | any | host DST_MAC) (IGMP-TYPE | ) (ip-precedence PRECEDENCE | dscp DSCP | ) (non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment) (routed-packet | ) (options | ) (packet-length OPERATOR LENGTH | ) (TIME_RANGE_NAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ILGP-TYPE</td>
<td>IGMP type</td>
<td></td>
</tr>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_MAC SRC_MAC_MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>any</td>
<td>Any source host</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_MAC</td>
<td>The source IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>DST_MAC DST_MAC_MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>host DST_MAC</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td>-</td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td>-</td>
</tr>
<tr>
<td>TIME_RANGE_NAME</td>
<td>The time-range used by the IP filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>
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
```

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
```

Related Commands
no sequence-num

11.4.20 permit gre

Command Purpose
Use this command to permit GRE packets matching the IP filter.

Command Syntax
```
(SEQUENCE_NUM | ) permit gre ( SRC_MAC SRC_MAC_MASK | any | host SRC_MAC | DST_MAC DST_MAC_MASK | any | host DST_MAC ) ( key KEY 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 | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEY</td>
<td>GRE key</td>
<td>0-4294967295</td>
</tr>
<tr>
<td>KEY-MASK</td>
<td>GRE key mask</td>
<td>0-0xFFFFFFFF</td>
</tr>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_MAC SRC_MAC_MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>any</td>
<td>Any source host</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_MAC</td>
<td>The source IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>DST_MAC DST_MAC_MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>host DST_MAC</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
</tbody>
</table>

www.fs.com
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td>-</td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td>-</td>
</tr>
<tr>
<td>TIME_RANGE_NAME</td>
<td>The time-range used by the IP filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**Command Mode**

IP ACL Configuration

**Default**

None

**Usage**

This type of filter is mostly used to permit GRE packets.

**Examples**

This example shows how to create a filter in IP ACL to permit any GRE packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 1 permit gre any any key 0 mask 0
```

This example shows how to create a filter in IP ACL to permit the GRE packets with the source IP address 1.1.1.1, any destination IP address and the gre key is 10:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 2 permit gre host 1.1.1.1 any key 10 mask 0xffffffff
```

**Related Commands**

no sequence-num

11.4.21 permit nvgre

**Command Purpose**

Use this command to permit NVGRE packets matching the IP filter.

**Command Syntax**

```plaintext
(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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSID</td>
<td>NVGRE vsid</td>
<td>0-16777215</td>
</tr>
<tr>
<td>VSID-MASK</td>
<td>NVGRE vsid mask</td>
<td>0-0xFFFFFFFF</td>
</tr>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_MAC SRC_MAC_MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>any</td>
<td>Any source host</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_MAC</td>
<td>The source IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>DST_MAC DST_MAC_MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>host DST_MAC</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td>-</td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td>-</td>
</tr>
<tr>
<td>TIME_RANGE_NAME</td>
<td>The time-range used by the IP filter</td>
<td>string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range.</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**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 0xffffffff

Related Commands

no sequence-num

11.4.22 show access-list ip

Command Purpose

Use this command to show the information of IP ACL.

Command Syntax

show access-list ip (ACL_NAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL_NAME</td>
<td>The name of the IP ACL</td>
<td>A string with up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to show the information of IP ACL:

Switch# show access-list ip
ip access-list list_ipv4_1
  2 permit tcp host 1.1.1.1 any
  3 deny icmp any any
  12 permit tcp any any

Related Commands

ip access-list
11.5 Extend ACL Commands

11.5.1 ip access-list extend

Command Purpose
Use this command to create extend IP ACL and then enter extend IP ACL configuration mode.
To remove this ACL, use the no form of this command.

Command Syntax
ip access-list ACL_NAME extend
no ip access-list ACL_NAME extend

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL_NAME</td>
<td>The name of an extend IP ACL</td>
<td>A string with up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
If the system already has an extend IP ACL with the same name, this command will enter the extend IP ACL configuration mode. However, if the ACL name is used by other type of ACL, a prompt message will be shown.
When the name is not used by any ACL, this command is to create an extend IP ACL firstly and then enter the extend IP ACL configuration mode.
On how to apply the created extend IP ACL in the interface, please refer to the usage of match access-group command in related chapter.

Examples
This example shows how to create an extend IP ACL named list_ipv4_1 and then enter the extend IP ACL configuration mode:

Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)#

This example shows how to remove the extend IP ACL named list_ipv4_1:

Switch# configure terminal
Switch(config)# no ip access-list list_ipv4_1 extend

Related Commands
match access-group

11.5.2 sequence-num

Command Purpose
Use this command to delete a filter from extend IP ACL.

Command Syntax
no sequence-num SEQUENCE_NUM
### Command Mode

**Extend IP ACL Configuration**

### Default

None

### Usage

None

### Examples

This example shows how to delete an IP or MAC filter with sequence number 10 from an extend IP ACL:

Switch# configure terminal  
Switch(config)# ip access-list list_ipv4_1 extend  
Switch(config-ex-ip-acl)# no sequence-num 10

### Related Commands

deny
deny udp
deny icmp
deny igmp
permit
permit tcp
permit udp
permit icmp
permit igmp
deny src-mac
permit src-mac

#### 11.5.3 deny src-mac

### Command Purpose

Use this command to create a filter for discarding ongoing packets matching the filter rule.

### Command Syntax

```
( SEQUENCE_NUM | ) deny src-mac ( any | MAC_ADDR MAC_ADDR_MASK | host MAC_ADDR ) ( dest-mac ( any | MAC_ADDR MAC_ADDR_MASK | host MAC_ADDR ) ) ( vlan VLAN_ID | ) ( cos COS | ) ( inner-vlan INNER_VLAN_ID | ) ( inner-cos INNER_COS | ) ( arp-packet ( | arp-op-code )
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>any</td>
<td>Any host</td>
<td>-</td>
</tr>
<tr>
<td>MAC_ADDR</td>
<td>The MAC address and its wildcard bits</td>
<td>MAC and wildcard in HHHH.HHHH.HHHH format</td>
</tr>
<tr>
<td>MAC_ADDR_MASK</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>host MAC_ADDR</td>
<td>The host with a specified MAC address</td>
<td>MAC address in HHHH.HHHH.HHHH format</td>
</tr>
<tr>
<td>dest-mac</td>
<td>Destination MAC address</td>
<td>-</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>VLAN-ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>COS</td>
<td>CoS</td>
<td>0-7</td>
</tr>
<tr>
<td>INNER_VLAN_ID</td>
<td>Inner VLAN-ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>INNER_COS</td>
<td>Inner CoS</td>
<td>0-7</td>
</tr>
<tr>
<td>arp-addr</td>
<td>ARP protocol</td>
<td>-</td>
</tr>
<tr>
<td>arp-op-code</td>
<td>arp-op-code</td>
<td>0-65535</td>
</tr>
<tr>
<td>sender-ip</td>
<td>sender-ip</td>
<td>-</td>
</tr>
<tr>
<td>target-ip</td>
<td>target-ip</td>
<td>-</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>The ip address and wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>host IP_ADDR</td>
<td>The host with a specified ip address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the extend IP filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

{ 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 | ) |

**Command Mode**

Extend IP ACL Configuration

**Default**

None

**Usage**

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the extend IP ACL. i.e. when the maximum existing sequence number is 100, the sequence number of subsequent created MAC filter is 110.
**Examples**

This example shows how to create a filter in extend IP ACL to deny the packets with source MAC address 001A.A02C.A1DF:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 1 deny src-mac host 001A.A02C.A1DF
```

This example shows how to create a filter in extend IP ACL to deny all the packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 2 deny src-mac any
```

This example shows how to create a filter in extend IP ACL to deny the packet whose source MAC address is between the ranges specified:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 3 deny src-mac 001A.A02C.A1DF 001A.A02C.0000
```

**Related Commands**

no sequence-num

**11.5.4 permit src-mac**

**Command Purpose**

Use this command to create a filter for allowing packets matching the filter rule to be delivered.

**Command Syntax**

```
( SEQUENCE_NUM | ) permit src-mac ( any | MAC_ADDR MAC_ADDR_MASK | host MAC_ADDR ) ( dest-mac ( any | MAC_ADDR MAC_ADDR_MASK | host MAC_ADDR ) | ) ) ( vlan VLAN_ID | ) ( cos VALUE | ) ( inner-vlan INNER_VLAN_ID | ) ( inner-cos INNER_COS | ) ( arp-packet ( | arp-op-code ) ( sender-ip ( IP_ADDR IP_ADDR_MASK | any | host IP_ADDR ) | ) ) ( target-ip ( IP_ADDR IP_ADDR_MASK | any | host IP_ADDR ) | ) ) | packet-length OPERATOR LENGTH | ( time-range TIME-RANGE-NAME | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>any</td>
<td>Any host</td>
<td>-</td>
</tr>
<tr>
<td>MAC_ADDR MAC_ADDR_MASK</td>
<td>The MAC address and its wildcard bits</td>
<td>MAC and wildcard in HHHH.HHHH.HHHH format</td>
</tr>
<tr>
<td>host MAC_ADDR</td>
<td>The host with a specified MAC address</td>
<td>MAC address in HHHH.HHHH.HHHH format</td>
</tr>
<tr>
<td>dest-mac</td>
<td>Destination MAC address</td>
<td>-</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>VLAN-ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>COS</td>
<td>CoS</td>
<td>0-7</td>
</tr>
<tr>
<td>INNER_VLAN_ID</td>
<td>Inner VLAN-ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>INNER_COS</td>
<td>Inner CoS</td>
<td>0-7</td>
</tr>
<tr>
<td>arp</td>
<td>ARP protocol</td>
<td>-</td>
</tr>
<tr>
<td>arp-op-code</td>
<td>arp-op-code</td>
<td>0-65535</td>
</tr>
<tr>
<td>Parameter</td>
<td>Parameter Description</td>
<td>Parameter Value</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>sender-ip</td>
<td>sender-ip</td>
<td>-</td>
</tr>
<tr>
<td>target-ip</td>
<td>target-ip</td>
<td>-</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>The ip address and wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>IP_ADDR_MASK</td>
<td>The host with a specified ip address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the extend IP filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**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-ac)# 3 permit src-mac 001A.A02C.A1DF 001A.A02C.0000
```

**Related Commands**

no sequence-num

**11.5.5 deny**

**Command Purpose**

Use this command to discard ongoing IP packets matching the IP filter.

**Command Syntax**

```
(SEQUENCE_NUM | ) deny ( PROTO_NUM | any ) ( SRC_IP SRC_IP_MASK | any | host SRC_IP ) ( DST_IP DST_IP_MASK | any | host DST_IP ) (ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment | ( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of the filter in IP ACL. An auto-generated sequence number will be</td>
<td>1-131071</td>
</tr>
<tr>
<td></td>
<td>assigned to the filter if this field is not presented.</td>
<td></td>
</tr>
<tr>
<td>PROTO_NUM</td>
<td>An IP protocol number, the range is 0 to 255</td>
<td>Agreement Number</td>
</tr>
<tr>
<td>any</td>
<td>Any protocol</td>
<td></td>
</tr>
<tr>
<td>SRC_IP SRC_IP_MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>host SRC_IP</td>
<td>The source IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>DST_IP DST_IP_MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>host DST_IP</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td></td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td></td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td></td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td></td>
</tr>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td></td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td></td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td></td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and</td>
<td>eq (equal to), lt (less than),</td>
</tr>
<tr>
<td></td>
<td>range</td>
<td>gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**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(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 1 deny any any
```

This example shows how to create a filter in extend IP ACL to deny the fragment packets with the source IP address 1.1.1.1:

```
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 2 deny any host 1.1.1.1 any fragments
```

This example shows how to create a filter in extend IP ACL to deny any routed packets:

```
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 3 deny any any any routed-packet
```

Related Commands

no sequence-num

11.5.6 deny tcp

Command Purpose

Use this command to reject TCP packets matching the IP filter.

Command Syntax

```
( SEQUENCE_NUM | ) deny tcp ( SRC_IP SRC_IP_MASK | any | host SRC_IP ) ( src-port OPERATOR SRC_PORT | ) ( DST_IP DST_IP_MASK | any | host DST_IP ) ( dst-port OPERATOR DST_PORT | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( established | ( match-any | match-all FLAG-NAME | ) ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment | routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_IP SRC_IP_MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>any</td>
<td>Any source host</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_IP</td>
<td>The source IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>OPERATOR SRC_PORT</td>
<td>Source port operator and value</td>
<td>Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>DST_IP DST_IP_MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>host DST_IP</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>Parameter</td>
<td>Parameter Description</td>
<td>Parameter Value</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>OPERATOR DST_PORT</td>
<td>Destination port operator and value</td>
<td>Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>established</td>
<td>Match established connections</td>
<td>-</td>
</tr>
<tr>
<td>match-any</td>
<td>Match any of the flag-name</td>
<td>-</td>
</tr>
<tr>
<td>FLAG-NAME</td>
<td>Match all the flag-name, including ack, fin, psh, rst, syn and urg</td>
<td>ack, fin, psh, rst, syn and urg</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td>-</td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td>-</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the IP filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR LENGTH</td>
<td>Packet length operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**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
```

This example shows how to create a filter in extend IP ACL to deny the TCP packets with the source IP address 1.1.1.1, source port 0-100:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 2 deny tcp host 1.1.1.1 src-port range 0 100 any
```
This example shows how to create a filter in extend IP ACL to deny any TCP packets in established TCP streams:

Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 3 deny tcp any any established

This example shows how to create a filter in extend IP ACL to deny the TCP ACK packets with the source IP address 10.10.10.0:

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

Related Commands
no sequence-num

11.5.7 deny udp

Command Purpose
Use this command to reject UDP packets matching the IP filter.

Command Syntax
(SEQUENCE_NUM |) deny udp (SRC_IP SRC_IP_MASK | any | host SRC_IP | (src-port OPERATOR SRC_PORT |)) (DST_IP DST_IP_MASK | any | host DST_IP | (dst-port OPERATOR DST_PORT |)) (ip-precedence PRECEDENCE | dscp DSCP |) (non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment | routed-packet | | options |) (packet-length OPERATOR LENGTH |) (time-range TIME-RANGE-NAME |)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_IP SRC_IP_MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>any</td>
<td>Any source host</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_IP</td>
<td>The source IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>OPERATOR SRC_PORT</td>
<td>Source port operator and value</td>
<td>Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>DST_IP DST_IP_MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>host DST_IP</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>OPERATOR DST_PORT</td>
<td>Destination port operator and value</td>
<td>Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td>-</td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td>-</td>
</tr>
</tbody>
</table>
### 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:

```plaintext
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:

```plaintext
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 2 deny udp host 1.1.1.1 src-port eq 10 any dst-port lt 2000
```

### Related Commands

no sequence-num

### 11.5.8 deny icmp

### Command Purpose

Use this command to reject ICMP packets matching the IP filter.

#### Command Syntax

```plaintext
(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 | )
```

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td>-</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the IP filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
<tr>
<td>Parameter</td>
<td>Parameter Description</td>
<td>Parameter Value</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>TYPE-NUM</td>
<td>ICMP message type</td>
<td>0-255</td>
</tr>
<tr>
<td>CODE-NUM</td>
<td>ICMP message code</td>
<td>0-255</td>
</tr>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_IP SRC_IP_MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>any</td>
<td>Any source IP address</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_IP</td>
<td>The source IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>DST_IP DST_IP_MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>host DST_IP</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td>-</td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td>-</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**Command Mode**
Extend IP ACL Configuration

**Default**
None
Usage
None

Examples
This example shows how to create a filter in extend IP ACL to deny any UDP packets:

Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 1 deny udp any

This example shows how to create a filter in extend IP ACL to deny the UDP packets with the source IP 1.1.1.1, source port 10, and destination port less than 2000:

Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 2 deny udp host 1.1.1.1 src-port eq 10 any dst-port lt 2000

Related Commands
no sequence-num

11.5.9 deny igmp

Command Purpose
Use this command to reject IGMP packets matching the IP filter.

Command Syntax
( SEQUENCE_NUM | ) deny igmp ( SRC_IP SRC_IP_MASK | any | host SRC_IP ) ( DST_IP DST_IP_MASK | any | host DST_IP ) ( IGMP-TYPE | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | ) ( options ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP-TYPE</td>
<td>IGMP type</td>
<td>including dvmrp, host-query, host-report, mtrace, mtrace-response, pim, precedence, trace, v2-leave, v2-report, v3-report</td>
</tr>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_IP SRC_IP_MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>any</td>
<td>Any source IP address</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_IP</td>
<td>The source IP address of a host</td>
<td>-</td>
</tr>
<tr>
<td>DST_IP DST_IP_MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>host DST_IP</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>Parameter</td>
<td>Parameter Description</td>
<td>Parameter Value</td>
</tr>
<tr>
<td>----------------</td>
<td>------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td></td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td></td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td></td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td></td>
</tr>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td></td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td></td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td></td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**Command Mode**

Extend IP ACL Configuration

**Default**

None

**Usage**

None

**Examples**

This example shows how to create a filter in extend IP ACL to deny any ICMP packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 1 deny icmp any any
```

This example shows how to create a filter in extend IP ACL to deny the ICMP packets with the icmp-type 3 and icmp-code 3:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 2 deny icmp any any icmp-type 3 icmp-code 3
```

**Related Commands**

no sequence-num
11.5.10  deny gre

**Command Purpose**

Use this command to reject GRE packets matching the IP filter.

**Command Syntax**

```
( SEQUENCE_NUM | ) deny gre ( SRC_IP SRC_IP_MASK | any | host SRC_IP ) ( DST_IP DST_IP_MASK | any | host DST_IP ) ( key KEY mask KEY-MASK ) ( ip-precedence PRECEDENCE | dscp DSCP ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment | routed-packet ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEY</td>
<td>GRE key</td>
<td>0-4294967295</td>
</tr>
<tr>
<td>KEY-MASK</td>
<td>GRE key mask</td>
<td>0-0xFFFFFFFF</td>
</tr>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_IP SRC_IP MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>any</td>
<td>Any source IP address</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_IP</td>
<td>The source IP address of a host</td>
<td>-</td>
</tr>
<tr>
<td>DST_IP DST_IP Mask</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>host DST_IP</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td>-</td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td>-</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>
Command Mode
Extend IP ACL Configuration

Default
None

Usage
This type of filter is mostly used to reject GRE packets.

Examples
This example shows how to create a filter in extend IP ACL to deny any IGMP packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 1 deny igmp any any
```

This example shows how to create a filter in extend IP ACL to deny the IGMP packets with the source IP address 1.1.1.1, any destination IP address and the igmp-type pim:

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

Related Commands
no sequence-num

11.5.11 deny nvgre

Command Purpose
Use this command to reject NVGRE packets matching the IP filter.

Command Syntax

```
(SEQUENCE_NUM |) deny nvgre (SRC_IP SRC_IP_MALE | any | host SRC_IP | DST_IP DST_IP_MALE | 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 |)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSID</td>
<td>NVGRE vsid</td>
<td>0-16777215</td>
</tr>
<tr>
<td>VSID-MASK</td>
<td>NVGRE vsid mask</td>
<td>0-0xFFFFFFFF</td>
</tr>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_IP SRC_IP_MALE</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>any</td>
<td>Any source IP address</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_IP</td>
<td>The source IP address of a host</td>
<td>-</td>
</tr>
<tr>
<td>Parameter</td>
<td>Parameter Description</td>
<td>Parameter Value</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>DST_IP DST_IP_MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>host DST_IP</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td>-</td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td>-</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**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 0 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`

### 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 | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>PROTO_NUM</td>
<td>An IP protocol number, the range is 0 to 255</td>
<td>0-255</td>
</tr>
<tr>
<td>SRC_IP SRC_IP_MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>host SRC_IP</td>
<td>The source IP address of a host</td>
<td>-</td>
</tr>
<tr>
<td>DST_IP DST_IP_MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>host DST_IP</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td>-</td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td>-</td>
</tr>
</tbody>
</table>
### 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 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 0xffffffff
```

This example shows how to create a filter in extend IP ACL to permit any routed packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 30 permit any any routed-packet
```

### Related Commands

no sequence-num

11.5.13 permit tcp

### Command Purpose

Use this command to permit TCP packets matching the IP filter.
### Command Syntax

```plaintext
(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 |)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_IP SRC_IP_MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>any</td>
<td>Any source host</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_IP</td>
<td>The source IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>OPERATOR SRC_PORT</td>
<td>Source port operator and value</td>
<td>Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>DST_IP DST_IP_MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>host DST_IP</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>OPERATOR DST_PORT</td>
<td>Destination port operator and value</td>
<td>Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>established</td>
<td>Match established connections</td>
<td>-</td>
</tr>
<tr>
<td>match-any</td>
<td>Match any of the flag-name</td>
<td>-</td>
</tr>
<tr>
<td>FLAG-NAME</td>
<td>Match all the flag-name, including ack, f in, psh, rst, syn and urg</td>
<td>ack, fin, psh, rst, syn and urg</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td>-</td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td>-</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the IP filter</td>
<td>-</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>
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
```

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

11.5.14 permit udp

Command Purpose
Use this command to permit UDP packets when the packets match this access-list.

Command Syntax
```
(SEQUENCE_NUM | ) permit udp (SRC_IP SRC_IP MASK | any | host SRC_IP ) (src-port OPERATOR SRC_PORT | ) (DST_IP DST_IP MASK | any host DST_IP | ) ( dst-port OPERATOR DST_PORT | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_IP SRC_IP_MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>any</td>
<td>Any source host</td>
<td></td>
</tr>
<tr>
<td>host SRC_IP</td>
<td>The source IP address of a host</td>
<td>Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>OPERATOR SRC_PORT</td>
<td>Source port operator and value</td>
<td></td>
</tr>
<tr>
<td>DST_IP DST_IP_MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>host DST_IP</td>
<td>The destination IP address of a host</td>
<td>Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>OPERATOR DST_PORT</td>
<td>Destination port operator and value</td>
<td></td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td></td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td></td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td></td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td></td>
</tr>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td></td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td></td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td></td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the IP filter</td>
<td></td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td></td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**Command Mode**

Extend IP ACL Configuration
Default
None

Usage
The fragments will be invalid when the layer 4 information is specified (i.e. src-port).

Examples
This example shows how to create a filter in extend IP ACL to deny any UDP packets:

Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 1 permit udp any any

This example shows how to create a filter in extend IP ACL to deny the UDP packets with the source IP address 1.1.1.1, source port 10, and destination port less than 2000:

Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 2 permit udp host 1.1.1.1 src-port eq 10 any dst-port lt 2000

Related Commands
no sequence-num

11.5.15 permit icmp

Command Purpose
Use this command to permit ICMP packets when the packets match this access-list.

Command Syntax

( SEQUENCE_NUM | ) permit icmp ( SRC_IP SRC_IP_MASS | 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 | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp-type TYPE-NUM</td>
<td>ICMP message type</td>
<td>0-255</td>
</tr>
<tr>
<td>icmp-code CODE-NUM</td>
<td>ICMP message code</td>
<td>0-255</td>
</tr>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_IP SRC_IP_MASS</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>any</td>
<td>Any source IP address</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_IP</td>
<td>The source IP address of a host</td>
<td>-</td>
</tr>
<tr>
<td>DST_IP DST_IP_MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>host DST_IP</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>Parameter</td>
<td>Parameter Description</td>
<td>Parameter Value</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td>-</td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td>-</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**Command Mode**

Extend IP ACL Configuration

**Default**

None

**Usage**

None

**Examples**

This example shows how to create a filter in extend IP ACL to permit any ICMP packets:

Switch# configure terminal  
Switch(config)# ip access-list list_ipv4_1 extend  
Switch(config-ex-ip-acl)# 1 permit icmp any any

This example shows how to create a filter in extend IP ACL to permit the ICMP packets with the icmp-type 3 and icmp-code 3:

Switch# configure terminal  
Switch(config)# ip access-list list_ipv4_1 extend  
Switch(config-ex-ip-acl)# 2 permit icmp any any icmp-type 3 icmp-code 3

**Related Commands**

None

**11.5.16 permit igmp**

**Command Purpose**

Use this command to permit IGMP packets matching the IP filter.
### Command Syntax

```
( SEQUENCE_NUM | ) permit igmp ( SRC_IP SRC_IP_MASK | any | host SRC_IP ) ( DST_IP DST_IP_MASK | any | host DST_IP ) ( IGMP-TYPE | )
( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment )
( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

### Parameter | Parameter Description | Parameter Value
--- | --- | ---
IGMP-TYPE | IGMP type | including dvmrp, host-query, host-report, mtrace, mtrace-response, pim, precedence, trace, v2-leave, v2-report, v3-report
SEQUENCE_NUM | The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented. | 1-131071
PROTO_NUM | An IP protocol number, the range is 0 to 255 | 0-255
any | Any protocol | -
SRC_IP | The source IP address | IPv4 Address and Mask
SRC_IP_MASK | The source IP address and its wildcard bits | IPv4 Address and Mask
DST_IP | The destination IP address | IPv4 Address
DST_IP_MASK | The destination IP address and its wildcard bits | IPv4 Address
host | 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-ext-ip-acl)# 1 permit igmp any any

This example shows how to create a filter in extend IP ACL to permit the IGMP packets with the source IP address 1.1.1.1, any destination IP address and the igmp-type pim:

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

Related Commands
no sequence-num

11.5.17 permit gre

Command Purpose
Use this command to permit GRE packets matching the IP filter.

Command Syntax
(SEQUENCE_NUM | ) permit gre (SRC_IP SRC_IP_MASK | any | host SRC_IP) (DST_IP DST_IP_MASK | any | host DST_IP) (key KEY key | KEY-MASK | mask 0-0xFFFFFFFF) (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 |)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEY</td>
<td>GRE key</td>
<td>0-4294967295</td>
</tr>
<tr>
<td>KEY-MASK</td>
<td>GRE key mask</td>
<td>0-0xFFFFFFFF</td>
</tr>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_IP SRC_IP_MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>any</td>
<td>Any source IP address</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_IP</td>
<td>The source IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>DST_IP DST_IP_MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>host DST_IP</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>Parameter</td>
<td>Parameter Description</td>
<td>Parameter Value</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td>-</td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td>-</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**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 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 10 mask 0xffffffff
```

**Related Commands**

- `no sequence-num`
- **11.5.18 permit nvgre**

**Command Purpose**

Use this command to permit NVGRE packets matching the IP filter.
### Command Syntax

```
(SEQUENCE_NUM |) permit nvgre (SRC_IP SRC_IP_MASK | any | host SRC_IP | (DST_IP DST_IP_MASK | any | host DST_IP | (vsid VSID | 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 |)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSID</td>
<td>NVGRE vsid</td>
<td>0-16777215</td>
</tr>
<tr>
<td>VSID-MASK</td>
<td>NVGRE vsid mask .</td>
<td>0-0xFFFFFFFF</td>
</tr>
<tr>
<td>SEQUENCE_NUM</td>
<td>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.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_IP</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>SRC_IP_MASK</td>
<td>The source IP address and its wildcard bits</td>
<td>IPv4 Address and Mask</td>
</tr>
<tr>
<td>DST_IP</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>DST_IP_MASK</td>
<td>The destination IP address and its wildcard bits</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>host DST_IP</td>
<td>The destination IP address of a host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PRECEDENCE</td>
<td>Match packets with given precedence value</td>
<td>0-7</td>
</tr>
<tr>
<td>DSCP</td>
<td>Match packets with given dscp value</td>
<td>0-63</td>
</tr>
<tr>
<td>non-fragment</td>
<td>Match packets with non fragment</td>
<td>-</td>
</tr>
<tr>
<td>first-fragment</td>
<td>Match packets with first fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-or-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>small-fragment</td>
<td>Match packets with small fragment</td>
<td>-</td>
</tr>
<tr>
<td>non-first-fragment</td>
<td>Match packets with non first fragment</td>
<td>-</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>options</td>
<td>Match packets with IP options</td>
<td>-</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>
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 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 0xffffffff

Related Commands
no sequence-num

11.5.19 remark

Command Purpose
Use this command to add remarks for the extend IP ACL.
To remove remarks from the extend IP ACL, use the no form of this command.

Command Syntax
remark REMARK
no remark

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>REMARK</td>
<td>The remarks of the extend IP ACL</td>
<td>A string with up to 100 characters</td>
</tr>
</tbody>
</table>

Command Mode
Extend IP ACL Configuration

Default
None

Usage
The remark is up to 100 characters.

Examples
This example shows how to add a remark to describe the extend IP ACL:
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# remark remark0flist1

This example shows how to remove the remark from the extend IP ACL:

Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# no remark

Related Commands

None

11.5.20  show access-list ip extend

Command Purpose
Use this command to show the information of extend IP ACL.

Command Syntax

```
show access-list ip (ACL_NAME extend | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL_NAME extend</td>
<td>The name of the extend IP ACL</td>
<td>A string with up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to show the information of extend IP ACL:

```
Switch# show access-list ip

ip access-list ex_ip_list_ipv4_1 extend
  2 permit tcp host 1.1.1.1 any
  3 deny icmp any any
  12 permit tcp any any
```

Related Commands

ip access-list extend
11.6 ACLv6 Commands

11.6.1 ipv6 access-list

Command Purpose
Use this command to create IPv6 ACL and then enter IPv6 ACL in global configuration mode.

Command Syntax
ipv6 access-list ACL_NAME
no ipv6 access-list ACL_NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL_NAME</td>
<td>The name of the IPv6 ACL</td>
<td>A string with up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
If the system already has an IPv6 ACL with the same name, this command will enter the IPv6 ACL configuration mode. However, if the ACL name is used by other type of ACL, a prompt message will be shown.

When the name is not used by any ACL, this command is to create the IPv6 ACL firstly and then enter the IPv6 ACL configuration mode.

Examples
This example shows how to create an IPv6 ACL named list_ipv6_1 and then enter the IPv6 ACL configuration mode:

Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)#

This example shows how to remove the IPv6 ACL named list_ipv6_1:

Switch# configure terminal
Switch(config)# no ipv6 access-list list_ipv6_1

Related Commands
match access-group

11.6.2 sequence-num

Command Purpose
Use this command to remove a filter from IPv6 ACL.

Command Syntax
no sequence-num SEQUENCE_NUM

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of a IPv6 filter</td>
<td>The range is 1 to 131071</td>
</tr>
</tbody>
</table>

Command Mode
IPv6 ACL Configuration
**remark**

**Command Purpose**

Use this command to add remarks for the IPv6 ACL.

To remove remarks of the IPv6 ACL, use the no form of this command.

**Command Syntax**

```
remark REMARK
```

```
no remark
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>REMARK</td>
<td>The remarks of the IPv6 ACL</td>
<td>String with up to 100 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

IPv6 ACL Configuration

**Default**

None

**Usage**

The remarks are up to 100 characters. The exceed parts will not be stored and will be truncated.

**Examples**

This example shows how to add a remark to describe the IPv6 ACL:
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# remark remark of List for ipv6

This example shows how to remove the remark of the IPv6 ACL:

Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# no remark

Related Commands
ipv6 access-list

11.6.4 deny

Command Purpose
Use this command to discard ongoing IPv6 packets matching the IPv6 filter.

Command Syntax
(SEQUENCE_NUM | deny (PROTO_NUM | any) (SRC_IPV6 SRC_IPV6_MASK | any | host SRC_IPV6) (DST_IPV6 DST_IPV6_MASK | any | host DST_IPV6) (routed-packet | (packet-length OPERATOR LENGTH) | (time-range TIME-RANGE-NAME))

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.</td>
<td>1-131071</td>
</tr>
<tr>
<td>PROTO_NUM</td>
<td>An IPv6 protocol number</td>
<td>0-255</td>
</tr>
<tr>
<td>any</td>
<td>Any IPv6 protocol</td>
<td>-</td>
</tr>
<tr>
<td>SRC_IPV6</td>
<td>The source IPv6 prefix address</td>
<td>IPv6 Address and mask length</td>
</tr>
<tr>
<td>SRC_IPV6_MASK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>host</td>
<td>The source IPv6 address of a host</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>DST_IPV6</td>
<td>The destination IPv6 prefix address</td>
<td>IPv6 Address and mask length</td>
</tr>
<tr>
<td>DST_IPV6_MASK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>host</td>
<td>The destination IPv6 address of a host</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the IPv6 filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

Command Mode
IPv6 ACL Configuration
Default
None

Usage
An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the IPv6 ACL. For example, when the maximum existing sequence number is 100, the sequence number of subsequent created IPv6 filter is 110.

Examples
This example shows how to create a filter in IPv6 ACL to deny any IPv6 packets:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-ac)# 1 deny any any
```

This example shows how to create a filter in IPv6 ACL to deny any routed packets:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-ac)# 2 deny any any any routed-packet
```

Related Commands
no sequence-num

11.6.5 deny tcp

Command Purpose
Use this command to reject TCP packets matching the IPv6 filter.

Command Syntax
```
( SEQUENCE_NUM | ) deny tcp ( SRC_IPV6 SRC_IPV6_MASK | any | host SRC_IPV6 ) ( src-port OPERATOR SRC_PORT | ) ( DST_IPV6 DST_IPV6_MASK | any | host DST_IPV6 ) ( dst-port OPERATOR DST_PORT | ) ( routed-packet | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_IPV6 SRC_IPV6_MASK</td>
<td>The source IPv6 prefix address</td>
<td>IPv6 Address and mask length</td>
</tr>
<tr>
<td>any</td>
<td>Any destination host</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_IPV6</td>
<td>The source IPv6 address of a host</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>OPERATOR SRC_PORT</td>
<td>Source port operator and value</td>
<td>Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>DST_IPV6 DST_IPV6_MASK</td>
<td>The destination IPv6 prefix address</td>
<td>IPv6 Address and mask length</td>
</tr>
<tr>
<td>host DST_IPV6</td>
<td>The destination IPv6 address of a host</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>packet-length OPERATOR</td>
<td>Source port operator and value</td>
<td>Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>Source port operator and value</td>
<td>Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>time-range TIME-RANGE-NAME</td>
<td>Source port operator and value</td>
<td>Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
</tbody>
</table>
### Command Mode

**IPv6 ACL Configuration**

### Default

None

### Usage

None

### Examples

This example shows how to create a filter in IPv6 ACL to deny any TCP packets:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 1 deny tcp any any
```

This example shows how to create a filter in IPv6 ACL to deny the TCP packets with the source IPv6 address 2001::2020, source port 8080:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 2 deny tcp host 2001::2020 src-port eq 8080 any
```

### Related Commands

- `no sequence-num`

### 11.6.6 deny udp

#### Command Purpose

Use this command to reject UDP packets matching the IPv6 filter.

#### Command Syntax

```
(SEQUENCE_NUM | ) deny udp (SRC_IPV6 SRC_IPV6_MASK | any | host SRC_IPV6) (src-port OPERATOR SRC_PORT | ) (DST_IPV6 DST_IPV6_MASK | any | host DST_IPV6) (dst-port OPERATOR DST_PORT | ) (routed-packet | ) (packet-length OPERATOR LENGTH | ) (time-range TIME-RANGE-NAME | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPERATOR DST_PORT</td>
<td>Destination port operator and value</td>
<td>Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the IPv6 filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SEQUENCE_NUM</strong></td>
<td>The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.</td>
</tr>
<tr>
<td><strong>SRC_IPV6 SRC_IPV6_MASK</strong></td>
<td>The source IPv6 prefix address and mask length</td>
</tr>
<tr>
<td>any</td>
<td>Any destination host</td>
</tr>
<tr>
<td><strong>host SRC_IPV6</strong></td>
<td>The source IPv6 address of a host</td>
</tr>
<tr>
<td><strong>OPERATOR SRC_PORT</strong></td>
<td>Source port operator and value</td>
</tr>
<tr>
<td><strong>DST_IPV6 DST_IPV6_MASK</strong></td>
<td>The destination IPv6 prefix address and mask length</td>
</tr>
<tr>
<td><strong>host DST_IPV6</strong></td>
<td>The destination IPv6 address of a host</td>
</tr>
<tr>
<td><strong>OPERATOR DST_PORT</strong></td>
<td>Destination port operator and value</td>
</tr>
<tr>
<td><strong>routed-packet</strong></td>
<td>Match routed packet</td>
</tr>
<tr>
<td><strong>TIME-RANGE-NAME</strong></td>
<td>The time-range used by the IPv6 filter</td>
</tr>
<tr>
<td><strong>OPERATOR</strong></td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td><strong>LENGTH</strong></td>
<td>The length value</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-131071</td>
</tr>
<tr>
<td>IPv6 Address and mask length</td>
</tr>
<tr>
<td>IPv6 Address</td>
</tr>
<tr>
<td>Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>IPv6 Address</td>
</tr>
<tr>
<td>Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>Match routed packet</td>
</tr>
<tr>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Command Mode**

IPv6 ACL Configuration

**Default**

None

**Usage**

None

**Examples**

This example shows how to create a filter in IPv6 ACL to deny any UDP packets:
This example shows how to create a filter in IPv6 ACL to deny the UDP packets with the source IPv6 address 2001::2020, source port 8080:

Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 1 deny udp any

Related Commands
no sequence-num
11.6.7 deny icmp

Command Purpose
Use this command to reject ICMP packets matching the IPv6 filter.

Command Syntax

```
( SEQUENCE_NUM | ) deny icmp ( SRC_IPV6 SRC_IPV6_MASK | any | host SRC_IPV6 ) ( DST_IPV6 DST_IPV6_MASK | any | host DST_IPV6 )
( icmp-type TYPE-NUM ( icmp-code CODE-NUM | ) | ) ( routed-packet | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TYPE-NUM</td>
<td>ICMP message type</td>
<td>0-255</td>
</tr>
<tr>
<td>CODE-NUM</td>
<td>ICMP message code</td>
<td>0-255</td>
</tr>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_IPV6 SRC_IPV6_MASK</td>
<td>The source IPv6 prefix address</td>
<td>IPv6 Address and mask length</td>
</tr>
<tr>
<td>any</td>
<td>Any source host</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_IPV6</td>
<td>The source IPv6 address of a host</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>DST_IPV6 DST_IPV6_MASK</td>
<td>The destination IPv6 prefix address</td>
<td>IPv6 Address and mask length</td>
</tr>
<tr>
<td>host DST_IPV6</td>
<td>The destination IPv6 address of a host</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the IPv6 filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

Command Mode
IPv6 ACL Configuration
Default
None

Usage
None

Examples
This example shows how to create a filter in IPv6 ACL to deny any ICMP packets:

Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 1 deny icmp any any

This example shows how to create a filter in IPv6 ACL to deny the ICMP packets with the icmp-type 3 and icmp-code 3:

Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 2 deny icmp any any icmp-type 3 icmp-code 3

Related Commands
no sequence-num

11.6.8 deny gre

Command Purpose
Use this command to reject GRE packets matching the IPv6 filter.

Command Syntax
```plaintext
(SEQUENCE_NUM | ) deny gre (SRC_IPV6 SRC_IPV6_MASK | any | host SRC_IPV6 ) ( DST_IPV6 DST_IPV6_MASK | any | host DST_IPV6 ) ( flow-label FLOW-LABEL-VALUE | ) ( key KEY mask KEY-MASK | ) ( dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment | routed-packet | | options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>FLOW-LABEL-VALUE</td>
<td>Flow label</td>
<td>0-1048575</td>
</tr>
<tr>
<td>KEY</td>
<td>GRE key</td>
<td>0-4294967295</td>
</tr>
<tr>
<td>KEY-MASK</td>
<td>GRE key mask</td>
<td>0-0xFFFFFFFF</td>
</tr>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of the filter in IPv6 ACL.</td>
<td>1-131071</td>
</tr>
<tr>
<td></td>
<td>An auto-generated sequence number will be</td>
<td></td>
</tr>
<tr>
<td></td>
<td>assigned to the filter if this field is not presented.</td>
<td></td>
</tr>
<tr>
<td>SRC_IPV6 SRC_IPV6_MASK</td>
<td>The source IPv6 prefix address</td>
<td>IPv6 Address and mask length</td>
</tr>
<tr>
<td>any</td>
<td>Any source host</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_IPV6</td>
<td>The source IPv6 address of a host</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>DST_IPV6 DST_IPV6_MASK</td>
<td>The destination IPv6 prefix address</td>
<td>IPv6 Address and mask length</td>
</tr>
<tr>
<td>host DST_IPV6</td>
<td>The destination IPv6 address of a host</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the IPv6 filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to),</td>
<td>eq (equal to), lt (less than),</td>
</tr>
<tr>
<td></td>
<td>lt (less than), gt (greater than), and range</td>
<td>gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>
Command Mode
IPv6 ACL Configuration

Default
None

Usage
None

Examples
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 1 deny gre any any 0 mask 0

Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 2 deny gre host 2000:1 any 10 mask 0xffffff

Related Commands
no sequence-num

11.6.9 deny nvgre

Command Purpose
Use this command to reject NVGRE packets matching the IPv6 filter.

Command Syntax
(SEQUENCE_NUM | ) deny nvgre ( SRC_IPV6 SRC_IPV6_MASK | any | host SRC_IPV6 ) ( DST_IPV6 DST_IPV6_MASK | any | host DST_IPV6 ) ( flow-label FLOW-LABEL-VALUE | ) ( vsid VSID mask VSID-MASK | discl 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 | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>FLOW-LABEL-VALUE</td>
<td>Flow label</td>
<td>0-1048575</td>
</tr>
<tr>
<td>VSID</td>
<td>NVGRE VSID</td>
<td>0-16777215</td>
</tr>
<tr>
<td>VSID-MASK</td>
<td>NVGRE VSID MASK</td>
<td>0-0xffffffff</td>
</tr>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_IPV6 SRC_IPV6_MASK</td>
<td>The source IPv6 prefix address</td>
<td>IPv6 Address and mask length</td>
</tr>
<tr>
<td>any</td>
<td>Any source host</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_IPV6</td>
<td>The source IPv6 address of a host</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>DST_IPV6 DST_IPV6_MASK</td>
<td>The destination IPv6 prefix address</td>
<td>IPv6 Address and mask length</td>
</tr>
<tr>
<td>host DST_IPV6</td>
<td>The destination IPv6 address of a host</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>Parameter</td>
<td>Parameter Description</td>
<td>Parameter Value</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the IPv6 filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**Command Mode**

IPv6 ACL Configuration

**Default**

None

**Usage**

None

**Examples**

Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ip6-acl)# 1 deny nvgre any any vsid 0 mask 0

Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ip6-acl)# 2 deny gre host 2000::1 any vsid 10 mask 0xffffffff

**Related Commands**

no sequence-num

**11.6.10 permit**

**Command Purpose**

Use this command to permit ongoing IPv6 packets matching the IPv6 filter.

**Command Syntax**

```
(SEQUENCE_NUM | ) permit ( PROTO_NUM | any ) ( SRC_IPV6 SRC_IPV6 MASK | any | host SRC_IPV6 ) ( DST_IPV6 DST_IPV6 MASK | any | host DST_IPV6 ) ( routed-packet | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.</td>
<td>1-131071</td>
</tr>
<tr>
<td>PROTO_NUM</td>
<td>An IPv6 protocol number</td>
<td>0-255</td>
</tr>
<tr>
<td>any</td>
<td>Any IPv6 protocol</td>
<td>-</td>
</tr>
<tr>
<td>Parameter</td>
<td>Parameter Description</td>
<td>Parameter Value</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td><strong>SRC_IPV6 SRC_IPV6_MAK</strong></td>
<td>The source IPv6 prefix address</td>
<td>IPv6 Address and mask length</td>
</tr>
<tr>
<td>host SRC_IPV6</td>
<td>The source IPv6 address of a host</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td><strong>DST_IPV6 DST_IPV6_MAK</strong></td>
<td>The destination IPv6 prefix address</td>
<td>IPv6 Address and mask length</td>
</tr>
<tr>
<td>host DST_IPV6</td>
<td>The destination IPv6 address of a host</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the IPv6 filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR LENGTH</td>
<td>Packet length, operator</td>
<td>eq (equal to), lt (less than),</td>
</tr>
<tr>
<td></td>
<td></td>
<td>gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**Command Mode**

IPv6 ACL Configuration

**Default**

None

**Usage**

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the IPv6 ACL. For example, when the maximum existing sequence number is 100, the sequence number of subsequent created IPv6 filter is 110.

**Examples**

This example shows how to create a filter in IPv6 ACL to permit any IPv6 packets:

```
Switch(config)## configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 1 permit any any
```

This example shows how to create a filter in IPv6 ACL to permit any routed packets:

```
Switch(config)# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 2 permit any any routed-packet
```

**Related Commands**

- **no sequence-num**
- **11.6.11 permit tcp**

**Command Purpose**

Use this command to permit TCP packets matching the IPv6 filter.

**Command Syntax**

```
(SEQUENCE_NUM | ) permit tcp ( SRC_IPV6 SRC_IPV6_MAK | any | host SRC_IPV6 ) ( src-port OPERATOR SRC_PORT | ) ( DST_IPV6 DST_IPV6_MAK | any | host DST_IPV6 ) ( dst-port OPERATOR DST_PORT | ) ( routed-packet | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_IPV6 SRC_IPV6_MASK</td>
<td>The source IPv6 prefix address IPv6 Address and mask length</td>
<td>Any destination host</td>
</tr>
<tr>
<td>host SRC_IPV6</td>
<td>The source IPv6 address of a host IPv6 Address</td>
<td>Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>OPERATOR SRC_PORT</td>
<td>Source port operator and value</td>
<td>Source port operator, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>DST_IPV6 DST_IPV6_MASK</td>
<td>The destination IPv6 prefix address IPv6 Address and mask length</td>
<td>Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>host DST_IPV6</td>
<td>The destination IPv6 address of a host IPv6 Address</td>
<td>Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>OPERATOR DST_PORT</td>
<td>Destination port operator and value</td>
<td>Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>Match routed packet</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the IPv6 filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**Command Mode**
IPv6 ACL Configuration

**Default**
None

**Usage**
None

**Examples**
This example shows how to create a filter in IPv6 ACL to permit any TCP packets:

Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config)# permit tcp any any
This example shows how to create a filter in IPv6 ACL to permit the TCP packets with the source IPv6 address 2001::2020, source port 8080:

Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 2 permit tcp host 2001::2020 src-port eq 8080 any

**Related Commands**

no sequence-num

**11.6.12 permit udp**

**Command Purpose**

Use this command to permit UDP packets matching the IPv6 filter.

**Command Syntax**

```
( SEQUENCE_NUM | ) permit udp ( SRC_IPV6 SRC_IPV6_MASK | any | host SRC_IPV6 ) ( src-port OPERATOR SRC_PORT | ) ( DST_IPV6 DST_IPV6_MASK | any | host DST_IPV6 ) ( dst-port OPERATOR DST_PORT | ) ( routed-packet | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_IPV6 SRC_IPV6_MASK</td>
<td>The source IPv6 prefix address IPv6 Address and mask length</td>
<td></td>
</tr>
<tr>
<td>any</td>
<td>Any destination host</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>host SRC_IPV6</td>
<td>The source IPv6 address of a host</td>
<td>Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>OPERATOR SRC_PORT</td>
<td>Source port operator and value</td>
<td></td>
</tr>
<tr>
<td>DST_IPV6 DST_IPV6_MASK</td>
<td>The destination IPv6 prefix address IPv6 Address and mask length</td>
<td></td>
</tr>
<tr>
<td>host DST_IPV6</td>
<td>The destination IPv6 address of a host</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>OPERATOR DST_PORT</td>
<td>Destination port operator and value</td>
<td>Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td></td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the IPv6 filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR LENGTH</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td></td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**Command Mode**

IPv6 ACL Configuration
Default

None

Usage

None

Examples

This example shows how to create a filter in IPv6 ACL to permit any UDP packets:

Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 1 permit udp any any

This example shows how to create a filter in IPv6 ACL to permit the UDP packets with the source IPv6 address 2001::2020, source port 8080:

Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 2 permit udp host 2001::2020 src-port eq 8080 any

Related Commands

no sequence-num

11.6.13 permit icmp

Command Purpose

Use this command to reject ICMP packets matching the IPv6 filter.

Command Syntax

( SEQUENCE_NUM | ) permit icmp ( SRC_IPV6 SRC_IPV6_MASK | any | host SRC_IPV6 ) ( DST_IPV6 DST_IPV6_MASK | any | host DST_IPV6 ) ( icmp-type TYPE-NUM { icmp-code CODE-NUM | | } { routed-packet | } { packet-length OPERATOR LENGTH | } { time-range TIME-RANGE-NAME | })

For other parameter descriptions, see the description in the "permit" section above.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp-type TYPE-NUM</td>
<td>ICMP message type</td>
<td>0-255</td>
</tr>
<tr>
<td>icmp-code CODE-NUM</td>
<td>ICMP message code</td>
<td>0-255</td>
</tr>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_IPV6 SRC_IPV6_MASK</td>
<td>The source IPv6 prefix address IPv6 Address and mask length</td>
<td></td>
</tr>
<tr>
<td>any</td>
<td>Any source host</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_IPV6</td>
<td>The source IPv6 address of a host IPv6 Address</td>
<td></td>
</tr>
<tr>
<td>DST_IPV6 DST_IPV6_MASK</td>
<td>The destination IPv6 prefix address IPv6 Address and mask length</td>
<td></td>
</tr>
<tr>
<td>host DST_IPV6</td>
<td>The destination IPv6 address of a host IPv6 Address</td>
<td></td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
</tbody>
</table>
### Command Mode

IPv6 ACL Configuration

**Default**
None

**Usage**
None

**Examples**

This example shows how to create a filter in IPv6 ACL to permit any ICMP packets:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 1 permit icmp any any
```

This example shows how to create a filter in IPv6 ACL to permit the ICMP packets with the icmp-type 3 and icmp-code 3:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 2 permit icmp any any icmp-type 3 icmp-code 3
```

**Related Commands**

- `no sequence-num`

### 11.6.14 permit gre

**Command Purpose**
Use this command to permit GRE packets matching the IPv6 filter.

**Command Syntax**

```
(SEQUENCE_NUM | ) permit gre ( SRC_IPV6 SRC_IPV6_MASK | any | host SRC_IPV6 ) ( DST_IPV6 DST_IPV6_MASK | any | host DST_IPV6 ) (flow-label FLOW-LABEL-VALUE | ) ( key KEY mask KEY-MASK ) ( dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment | ) ( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

For other parameter descriptions, see "deny gre" above.

---

**Parameter** | **Parameter Description** | **Parameter Value**
--- | --- | ---
**TIME-RANGE-NAME** | The time-range used by the IPv6 filter | A string with up to 40 characters
**OPERATOR** | Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range | eq (equal to), lt (less than), gt (greater than), and range
**LENGTH** | The length value | 64-16382
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>FLOW-LABEL-VALUE</td>
<td>Flow label</td>
<td>0-1048575</td>
</tr>
<tr>
<td>KEY</td>
<td>GRE key</td>
<td>0-4294967295</td>
</tr>
<tr>
<td>KEY-MASK</td>
<td>GRE key mask</td>
<td>0-0xFFFFFFFF</td>
</tr>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.</td>
<td>1-131071</td>
</tr>
<tr>
<td>SRC_IPV6 SRC_IPV6_MASK</td>
<td>The source IPv6 prefix address</td>
<td>IPv6 Address and mask length</td>
</tr>
<tr>
<td>any</td>
<td>Any source host</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_IPV6</td>
<td>The source IPv6 address of a host</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>DST_IPV6 DST_IPV6_MASK</td>
<td>The destination IPv6 prefix address</td>
<td>IPv6 Address and mask length</td>
</tr>
<tr>
<td>host DST_IPV6</td>
<td>The destination IPv6 address of a host</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the IPv6 filter</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range</td>
<td>eq (equal to), lt (less than), gt (greater than), and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

**Command Mode**

IPv6 ACL Configuration

**Default**

None

**Usage**

None

**Examples**

Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 1 permit gre any any key 0 mask 0

Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 2 permit gre host 2000::1 any key 10 mask 0xffffffff

**Related Commands**

no sequence-num
11.6.15  permit nvgre

Command Purpose
Use this command to permit NVGRE packets matching the IPv6 filter.

Command Syntax

( SEQUENCE_NUM | ) permit nvgre ( SRC_IPV6 SRC_IPV6_MASK | any | host SRC_IPV6 ) ( DST_IPV6 DST_IPV6_MASK | any | host DST_IPV6 ) ( flow-label FLOW-LABEL-VALUE | ) ( vsid VSID mask VSID-MASK ) ( dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment | ) ( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )

For other parameter descriptions, see "deny nvgre" above.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>FLOW-LABEL-VALUE</td>
<td>Flow label</td>
<td>0-1048575</td>
</tr>
<tr>
<td>VSID</td>
<td>NVGRE VSID</td>
<td>0-16777215</td>
</tr>
<tr>
<td>VSID-MASK</td>
<td>NVGRE VSID MASK</td>
<td>0-0xFFFFFFFF</td>
</tr>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of the</td>
<td>1-131071</td>
</tr>
<tr>
<td></td>
<td>filter in IPv6 ACL. An auto-</td>
<td></td>
</tr>
<tr>
<td></td>
<td>generated sequence number will</td>
<td></td>
</tr>
<tr>
<td></td>
<td>be assigned to the filter if</td>
<td></td>
</tr>
<tr>
<td></td>
<td>this field is not presented.</td>
<td></td>
</tr>
<tr>
<td>SRC_IPV6 SRC_IPV6_MASK</td>
<td>The source IPv6 prefix address</td>
<td>IPv6 Address and mask length</td>
</tr>
<tr>
<td>any</td>
<td>Any source host</td>
<td>-</td>
</tr>
<tr>
<td>host SRC_IPV6</td>
<td>The source IPv6 address of a</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td></td>
<td>host</td>
<td></td>
</tr>
<tr>
<td>DST_IPV6 DST_IPV6_MASK</td>
<td>The destination IPv6 prefix</td>
<td>IPv6 Address and mask length</td>
</tr>
<tr>
<td>host DST_IPV6</td>
<td>The destination IPv6 address</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td></td>
<td>of a host</td>
<td></td>
</tr>
<tr>
<td>routed-packet</td>
<td>Match routed packet</td>
<td>-</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the IPv6</td>
<td>A string with up to 40 characters</td>
</tr>
<tr>
<td></td>
<td>filter</td>
<td></td>
</tr>
<tr>
<td>OPERATOR</td>
<td>Packet length, operator</td>
<td>eq (equal to), lt</td>
</tr>
<tr>
<td></td>
<td>including eq (equal to),</td>
<td>(less than), gt</td>
</tr>
<tr>
<td></td>
<td>lt (less than), gt (greater</td>
<td>(greater than),</td>
</tr>
<tr>
<td></td>
<td>than), and range</td>
<td>and range</td>
</tr>
<tr>
<td>LENGTH</td>
<td>The length value</td>
<td>64-16382</td>
</tr>
</tbody>
</table>

Command Mode
IPv6 ACL Configuration

Default
None

Usage
None
Examples
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 1 permit nvgre any any vsid 0 mask 0
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 2 permit gre host 2000::1 any vsid 10 mask 0xffff

Related Commands
no sequence-num
show access-list ipv6

Command Purpose
Use this command to show the IPv6 ACL information.

Command Syntax
show access-list ipv6 ( ACL_NAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL_NAME</td>
<td>The name of the IPv6 ACL</td>
<td>A string with up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
If no ipv6 acl are specified, all ipv6 access-lists in the system should be shown.

Examples
This example shows how to show the IPv6 ACL information:
Switch# show access-list ipv6
ipv6 access-list list_ipv6_1
10 deny any 2001::/48 any
20 permit any any

Related Commands
ipv6 access-list

11.7 MPLS ACL Commands

11.7.1 mpls access-list

Command Purpose
Use this command to create MPLS ACL and then enter MPLS ACL in global configuration mode.

Command Syntax
mpls access-list ACL_NAME
no mpls access-list ACL_NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL_NAME</td>
<td>The name of the MPLS ACL</td>
<td>A string with up to 40 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

None

**Usage**

If the system already has an MPLS ACL with the same name, this command will enter the MPLS 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 MPLS ACL firstly and then enter the MPLS ACL Configuration mode.

**Examples**

This example shows how to create an MPLS named list_mpls_1 and then enter the MPLS ACL Configuration mode:

```
Switch# configure terminal
Switch(config)# mpls access-list list_mpls_1
Switch(config-mpls-acl)#
```

This example shows how to remove the MPLS ACL named list_mpls_1:

```
Switch# configure terminal
Switch(config)# no mpls access-list list_mpls_1
```

**Related Commands**

match access-group

11.7.2 sequence-num

**Command Purpose**

Use this command to remove a filter from MPLS ACL.

**Command Syntax**

no sequence-num SEQUENCE_NUM

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of a MPLS filter</td>
<td>1-131071</td>
</tr>
</tbody>
</table>

**Command Mode**

MPLS ACL Configuration

**Default**

None

**Usage**

None
Examples

This example shows how to remove a filter with the sequence-num 10 from MPLS ACL:

Switch# configure terminal
Switch(config)# mpls access-list list_mpls_1
Switch(config-mpls-acl)# no sequence-num 10

Related Commands
deny
permit

11.7.3 remark

Command Purpose
Use this command to add remarks for the MPLS ACL.
To remove remarks of the MPLS ACL, use the no form of this command.

Command Syntax
remark REMARK
no remark

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>REMARK</td>
<td>The remarks of the MPLS ACL</td>
<td>String with up to 100 characters</td>
</tr>
</tbody>
</table>

Command Mode
MPLS 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 MPLS ACL:

Switch# configure terminal
Switch(config)# mpls access-list list_mpls_1
Switch(config-mpls-acl)# remark remark of list for mpls

This example shows how to remove the remark of the MPLS ACL:

Switch# configure terminal
Switch(config)# mpls access-list list_mpls_1
Switch(config-mpls-acl)# no remark

Related Commands
mpls access-list

11.7.4 show access-list mpls

Command Purpose
Use this command to show the MPLS ACL information.
### Command Syntax

show access-list mpls (ACL_NAME |)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL_NAME</td>
<td>The name of the MPLS ACL</td>
<td>A string with up to 40 characters</td>
</tr>
</tbody>
</table>

### Command Mode

Privileged EXEC

### Default

None

### Usage

If no mpls acl are specified, all mpls access-lists in the system should be shown.

### Examples

This example shows how to show the MPLS ACL information:

```
Switch# show access-list mpls
mpls access-list mpls_1
  10 permit topmost-label 1 next-label 2
  20 deny topmost-label any
```

### Related Commands

mpls access-list

11.7.5 deny

### Command Purpose

Use this command to discard ongoing MPLS packets matching the MPLS filter.

### Command Syntax

(SEQUENCE_NUM |) deny topmost-label ( (MPLS-LABEL (mask MPLS-LABEL-MASK) | any) (exp EXP-VALUE |) (ttl TTL-VALUE |) next-label |)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of the filter in MPLS ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.</td>
<td>1-131071</td>
</tr>
<tr>
<td>topmost-label</td>
<td>mpls topmost label</td>
<td>-</td>
</tr>
<tr>
<td>next-label</td>
<td>mpls next label</td>
<td>-</td>
</tr>
<tr>
<td>MPLS-LABEL</td>
<td>mpls label value</td>
<td>0-1048575</td>
</tr>
<tr>
<td>MPLS-LABEL-MASK</td>
<td>mpls label mask</td>
<td>0-0xFFFFFFFF</td>
</tr>
<tr>
<td>EXP-VALUE</td>
<td>exp value</td>
<td>0-7</td>
</tr>
<tr>
<td>TTL-VALUE</td>
<td>ttl value</td>
<td>0-255</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the MPLS filter</td>
<td>A string with up to 40 characters</td>
</tr>
</tbody>
</table>
Command Mode
MPLS 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 MPLS ACL. For example, when the maximum existing sequence number is 100, the sequence number of subsequent created MPLS filter is 110.

Examples
This example shows how to create a filter in MPLS ACL to deny any MPLS packets:

Switch# configure terminal
Switch(config)# mpls access-list list_mpls_1
Switch(config-mpls-acl)# 1 deny topmost-label any

This example shows how to create a filter in MPLS ACL to deny any MPLS packets with first label is 1 and second label is 2:

Switch# configure terminal
Switch(config)# mpls access-list list_mpls_1
Switch(config-mpls-acl)# 2 deny topmost-label 1 next-label 2

Related Commands
no sequence-num
11.7.6 permit

Command Purpose
Use this command to permit ongoing MPLS packets matching the MPLS filter.

Command Syntax


<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.</td>
<td>1-131071</td>
</tr>
<tr>
<td>topmost-label</td>
<td>mpls topmost label</td>
<td>-</td>
</tr>
<tr>
<td>next-label</td>
<td>mpls next label</td>
<td>-</td>
</tr>
<tr>
<td>MPLS-LABEL</td>
<td>mpls label value</td>
<td>0-1048575</td>
</tr>
<tr>
<td>MPLS-LABEL-MASK</td>
<td>mpls label mask</td>
<td>0-0xFFFFF</td>
</tr>
<tr>
<td>EXP-VALUE</td>
<td>exp value</td>
<td>0-7</td>
</tr>
<tr>
<td>TTL-VALUE</td>
<td>ttl value</td>
<td>0-255</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the MPLS filter</td>
<td>A string with up to 40 characters</td>
</tr>
</tbody>
</table>
Command Mode
MPLS 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 MPLS ACL. For example, when the maximum existing sequence number is 100, the sequence number of subsequent created MPLS filter is 110.

Examples
This example shows how to create a filter in MPLS ACL to permit any MPLS packets:

```
Switch# configure terminal
Switch(config)# mpls access-list list_mpls_1
Switch(config-mpls-acl)# 1 permit topmost-label any
```

This example shows how to create a filter in MPLS ACL to permit any MPLS packets with first label is 1 and second label is 2:

```
Switch# configure terminal
Switch(config)# mpls access-list list_mpls_1
Switch(config-mpls-acl)# 2 permit topmost-label 1 next-label 2
```

Related Commands
no sequence-num

11.8 Extend MPLS ACL Commands

11.8.1 mpls access-list extend

Command Purpose
Use this command to create Extend MPLS ACL and then enter Extend MPLS ACL in global configuration mode.

Command Syntax

```
mpls access-list ACL_NAME extend
no mpls access-list ACL_NAME extend
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL_NAME</td>
<td>The name of the Extend MPLS ACL</td>
<td>A string with up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
If the system already has an Extend MPLS ACL with the same name, this command will enter the MPLS 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 Extend MPLS ACL firstly and then enter the Extend MPLS ACL configuration mode.
Examples

This example shows how to create an Extend MPLS ACL named list_ex_mpls_1 and then enter the Extend MPLS ACL configuration mode:

```
Switch# configure terminal
Switch(config)# mpls access-list list_ex_mpls_1 extend
Switch(config-ex-mpls-acl)#
```

This example shows how to remove the Extend MPLS ACL named list_ex_mpls_1:

```
Switch# configure terminal
Switch(config)# no mpls access-list list_ex_mpls_1 extend
```

Related Commands

match access-group

11.8.2 sequence-num

Command Purpose

Use this command to remove a filter from Extend MPLS ACL.

Command Syntax

```
no sequence-num SEQUENCE_NUM
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of a Extend MPLS filter</td>
<td>The range is 1 to 131071</td>
</tr>
</tbody>
</table>

Command Mode

Extended MPLS ACL Configuration

Default

None

Usage

None

Examples

This example shows how to remove a filter with the sequence-num 10 from Extend MPLS ACL:

```
Switch# configure terminal
Switch(config)# mpls access-list list_ex_mpls_1 extend
Switch(config-ex-mpls-acl)# no sequence-num 10
```

Related Commands

deny
permit

11.8.3 remark

Command Purpose

Use this command to add remarks for the Extend MPLS ACL.

To remove remarks of the Extend MPLS ACL, use the no form of this command.
Command Syntax
remark REMARK
no remark

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>REMARK</td>
<td>The remarks of the Extend MPLS ACL</td>
<td>String with up to 100 characters</td>
</tr>
</tbody>
</table>

Command Mode
Extended MPLS 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 Extend MPLS ACL:

Switch# configure terminal
Switch(config)# mpls access-list list_ex_mpls_1 extend
Switch(config-ex-mpls-acl)# remark remark of List for mpls

This example shows how to remove the remark of the Extend MPLS ACL:

Switch# configure terminal
Switch(config)# mpls access-list list_ex_mpls_1 extend
Switch(config-ex-mpls-acl)# no remark

Related Commands
mpls access-list

11.8.4 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 | ) ( time-range TIME-RANGE-NAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of the filter in Extend MPLS ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.</td>
<td>1-131071</td>
</tr>
<tr>
<td>any</td>
<td>Any host</td>
<td>-</td>
</tr>
<tr>
<td>MAC_ADDR MAC_ADDR_MASK</td>
<td>The MAC address and its wildcard bits</td>
<td>The MAC address and wildcard bits</td>
</tr>
<tr>
<td>Parameter</td>
<td>Parameter Description</td>
<td>Parameter Value</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>host MAC_ADDR</td>
<td>The host with a specified MAC address</td>
<td>MAC address</td>
</tr>
<tr>
<td>dest-mac</td>
<td>Destination MAC address</td>
<td>The MAC address and wildcard bits</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>VLAN-ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>COS</td>
<td>CoS</td>
<td>0-7</td>
</tr>
<tr>
<td>INNER_VLAN_ID</td>
<td>Inner VLAN-ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>INNER_COS</td>
<td>Inner CoS</td>
<td>0-7</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the MAC filter</td>
<td>A string with up to 40 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Extended MPLS 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 MPLS 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 MPLS ACL to deny the packets with source MAC address 001A.A02C.A1DF:

Switch# configure terminal
Switch(config)# mpls access-list list_ex_mpls_1 extend
Switch(config-ex-mpls-acl)# 1 deny src-mac host 001A.A02C.A1DF

This example shows how to create a filter in extend MPLS ACL to deny all the packets:

Switch# configure terminal
Switch(config)# mpls access-list list_ex_mpls_1 extend
Switch(config-ex-mpls-acl)# 2 deny src-mac any

This example shows how to create a filter in extend MPLS ACL to deny the packet whose source MAC address is between the ranges specified:

Switch# configure terminal
Switch(config)# mpls access-list list_ex_mpls_1 extend
Switch(config-ex-mpls-acl)# 3 deny src-mac 001A.A02C.A1DF 001A.A02C.0000

**Related Commands**

no sequence-num

11.8.5 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 | )
(time-range TIME-RANGE-NAME | )
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of the filter in Extend MPLS ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.</td>
<td>1-131071</td>
</tr>
<tr>
<td>any</td>
<td>Any host</td>
<td>-</td>
</tr>
<tr>
<td>MAC_ADDR MAC_ADDR_MASK</td>
<td>The MAC address and its wildcard bits</td>
<td>The MAC address and wildcard bits</td>
</tr>
<tr>
<td>host MAC_ADDR</td>
<td>The host with a specified MAC address</td>
<td>MAC address</td>
</tr>
<tr>
<td>dest-mac</td>
<td>Destination MAC address</td>
<td>The MAC address and wildcard bits</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>VLAN-ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>COS</td>
<td>CoS</td>
<td>0-7</td>
</tr>
<tr>
<td>INNER_VLAN_ID</td>
<td>Inner VLAN-ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>INNER_COS</td>
<td>Inner CoS</td>
<td>0-7</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the MAC filter</td>
<td>A string with up to 40 characters</td>
</tr>
</tbody>
</table>

**Command Mode**
Extended MPLS 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 MPLS 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 MPLS ACL to permit the packets with source MAC address 001A.A02C.A1DF:

```bash
Switch# configure terminal
Switch(config)# mpls access-list list_ex_mpls_1 extend
Switch(config-ex-mpls-ac)# 1 permit src-mac host 001A.A02C.A1DF
```

This example shows how to create a filter in extend MPLS ACL to permit all the packets:

```bash
Switch# configure terminal
Switch(config)# mpls access-list list_ex_mpls_1 extend
Switch(config-ex-mpls-ac)# 2 permit src-mac any
```

This example shows how to create a filter in extend MPLS ACL to permit the packets with source MAC address between the ranges specified:

```bash
Switch# configure terminal
Switch(config)# mpls access-list list_ex_mpls_1 extend
Switch(config-ex-mpls-ac)# 3 permit src-mac 001A.A02C.A1DF 001A.A02C.0000
```
Related Commands

- no sequence-num
- 11.8.6 deny

Command Purpose

Use this command to discard ongoing MPLS packets matching the Extend MPLS filter.

Command Syntax

```
(SEQUENCE_NUM |) deny topmost-label ((MPLS-LABEL (mask MPLS-LABEL-MASK) |) any) (exp EXP-VALUE |) (ttl TTL-VALUE |) next-label |)
((MPLS-LABEL (mask MPLS-LABEL-MASK) |) any) (exp EXP-VALUE |) (ttl TTL-VALUE |) next-label |) (MPLS-LABEL (mask MPLS-LABEL-MASK |) | any) (exp EXP-VALUE |) (ttl TTL-VALUE |) (stack-bottom |) (time-range TIME-RANGE-NAME |)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of the filter in Extend MPLS ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.</td>
<td>1-131071</td>
</tr>
<tr>
<td>topmost-label</td>
<td>mpls topmost label</td>
<td>-</td>
</tr>
<tr>
<td>next-label</td>
<td>mpls next label</td>
<td>-</td>
</tr>
<tr>
<td>MPLS-LABEL</td>
<td>mpls label value</td>
<td>0-1048575</td>
</tr>
<tr>
<td>MPLS-LABEL-MASK</td>
<td>mpls label mask</td>
<td>0-0xFFFFFFFF</td>
</tr>
<tr>
<td>EXP-VALUE</td>
<td>exp value</td>
<td>0-7</td>
</tr>
<tr>
<td>TTL-VALUE</td>
<td>ttl value</td>
<td>0-255</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the MPLS filter</td>
<td>A string with up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode

Extended MPLS 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 MPLS ACL. For example, when the maximum existing sequence number is 100, the sequence number of subsequent created Extend MPLS filter is 110.

Examples

This example shows how to create a filter in Extend MPLS ACL to deny any MPLS packets:

```
Switch# configure terminal
Switch(config)# mpls access-list list_ex_mpls_1 extend
Switch(config-ex-mpls-acl)# 1 deny topmost-label any
```

This example shows how to create a filter in Extend MPLS ACL to deny any MPLS packets with first label is 1 and second label is 2:

```
Switch# configure terminal
Switch(config)# mpls access-list list_ex_mpls_1 extend
Switch(config-ex-mpls-acl)# 2 deny topmost-label 1 next-label 2
```
Related Commands

no sequence-num

11.8.7 permit

Command Purpose

Use this command to permit ongoing MPLS packets matching the Extend MPLS filter.

Command Syntax

(SEQUENCE_NUM |) deny topmost-label ( MPLS-LABEL ( mask MPLS-LABEL-MASK ) | any ) ( exp EXP-VALUE | ) ( ttl TTL-VALUE | ) next-label | )
( ( MPLS-LABEL ( mask MPLS-LABEL-MASK ) | any ) ( exp EXP-VALUE | ) ( ttl TTL-VALUE | ) next-label | )
( ( MPLS-LABEL ( mask MPLS-LABEL-MASK ) | any ) ( exp EXP-VALUE | ) ( ttl TTL-VALUE | ) next-label | )
( stack-bottom | ) ( time-range TIME-RANGE-NAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQUENCE_NUM</td>
<td>The sequence number of the filter in Extend MPLS ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.</td>
<td>1-131071</td>
</tr>
<tr>
<td>topmost-label</td>
<td>mpls topmost label</td>
<td>-</td>
</tr>
<tr>
<td>next-label</td>
<td>mpls next label</td>
<td>-</td>
</tr>
<tr>
<td>MPLS-LABEL</td>
<td>mpls label value</td>
<td>0-1048575</td>
</tr>
<tr>
<td>MPLS-LABEL-MASK</td>
<td>mpls label mask</td>
<td>0-0xFFFFF</td>
</tr>
<tr>
<td>EXP-VALUE</td>
<td>exp value</td>
<td>0-7</td>
</tr>
<tr>
<td>TTL-VALUE</td>
<td>ttl value</td>
<td>0-255</td>
</tr>
<tr>
<td>TIME-RANGE-NAME</td>
<td>The time-range used by the MPLS filter</td>
<td>A string with up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode

Extended MPLS 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 MPLS ACL. For example, when the maximum existing sequence number is 100, the sequence number of subsequent created Extend MPLS filter is 110.

Examples

This example shows how to create a filter in Extend MPLS ACL to permit any MPLS packets:

Switch# configure terminal
Switch(config)# mpls access-list list_ex_mpls_1 extend
Switch(config-ex-mpls-acl)# 1 permit topmost-label any

This example shows how to create a filter in Extend MPLS ACL to permit any MPLS packets with first label is 1 and second label is 2:

Switch# configure terminal
Switch(config)# mpls access-list list_ex_mpls_1 extend
Switch(config-ex-mpls-acl)# 2 permit topmost-label 1 next-label 2
Related Commands

no sequence-num

11.8.8 show access-list mpls extend

Command Purpose
Use this command to show the Extend MPLS ACL information.

Command Syntax

show access-list mpls (ACL_NAME extend | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL_NAME</td>
<td>The name of the Extend MPLS ACL</td>
<td>A string with up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
If no mpls acl are specified, all mpls access-lists in the system should be shown.

Examples
This example shows how to show the Extend MPLS ACL information:

```
Switch# show access-list mpls
mpls access-list list_ex_mpls_1 extend
  10 permit topmost-label 1 next-label 2
  20 deny topmost-label any
```

Related Commands
mpls access-list extend

11.9 IEEE 802.1x Commands

11.9.1 dot1x system-auth-ctrl

Command Purpose
Use the dot1x system-auth-ctrl to globally start the dot1x authenticate control feature.
To remove this configure, use no form of this command.

Command Syntax
dot1x system-auth-ctrl
no dot1x system-auth-ctrl

Command Mode
Global Configuration
Default

Disable

Usage

Use this command to globally start the dot1x feature. To make the dot1x configures on each port work normally, this command should be used.

Examples

The following is sample output from the dot1x system-auth-ctrl command:

```
Switch# configure terminal
Switch(config)# dot1x system-auth-ctrl
Switch(config)# no dot1x system-auth-ctrl
```

Related Commands

show dot1x

dot1x port-control

11.9.2 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Specify the interface name to be initialized</td>
<td>This function supports routed port and access port, and Does not Support trunk port</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to initialize the IEEE 802.1x state machines and to set up a fresh environment for authentication. After you enter this command, the port status becomes unauthorized.

Examples

The following is sample output from the dot1x initialize command:

```
Switch# dot1x initialize interface eth-0-1
```

Related Commands

show dot1x
11.9.3 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>COUNT</td>
<td>Number of times that the switch restarts the authentication process before the port changes to the unauthorized state.</td>
<td>1-10</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
The default value of dot1x max-reauth-req is 2 times.

Usage
You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Examples
The following is sample output from the dot1x max-reauth-req command:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dot1x max-req 4
```

Related Commands
show dot1x

11.9.4 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
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>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</td>
<td>-</td>
</tr>
<tr>
<td>force-authorized</td>
<td>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</td>
<td>-</td>
</tr>
<tr>
<td>force-unauthorized</td>
<td>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</td>
<td>-</td>
</tr>
<tr>
<td>dir</td>
<td>Specify the dot1x control direction</td>
<td>-</td>
</tr>
<tr>
<td>both</td>
<td>Discard received and transmitted packets</td>
<td>-</td>
</tr>
<tr>
<td>in</td>
<td>Discard received packets only</td>
<td>-</td>
</tr>
</tbody>
</table>

**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:

```plaintext
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dot1x port-control auto
```
**Related Commands**

show dot1x

**11.9.5 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VER</td>
<td>The EAPOL version</td>
<td>1-2</td>
</tr>
</tbody>
</table>

**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:

```bash
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dot1x protocol-version 1
```

**Related Commands**

show dot1x

**11.9.6 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>The time interval (in seconds) between the retrials of authentication</td>
<td>1-65535 seconds</td>
</tr>
</tbody>
</table>

**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
dot1x

11.9.7  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
do 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
dot1x
dot1x timeout

11.9.8  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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>The interface to re-authenticate</td>
<td>This function supports routed port and access port, and Does not Support trunk port</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

You can use this command to re-authenticate a client without waiting for the configured number of seconds between re-authentication attempts (re-authperiod) and automatic re-authentication.

Examples

The following is sample output from the `dot1x re-authenticate` command:

```
Switch# dot1x re-authenticate interface eth-0-1
```

Related Commands

`show dot1x`

11.9.9 `dot1x timeout`

Command Syntax

```
dot1x timeout ( re-authperiod SECONDS | server-timeout SECONDS | supp-timeout SECONDS | tx-period SECONDS )
```

```
no dot1x timeout ( reauth-period | server-timeout | supp-timeout | tx-period )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>re-authperiod SECONDS</td>
<td>Set the number of seconds between reauthentication attempts.</td>
<td>60-65535 seconds</td>
</tr>
<tr>
<td>server-timeout SECONDS</td>
<td>Number of seconds that the switch waits for the retransmission of packets by the switch to the authentication server.</td>
<td>1-65535 seconds</td>
</tr>
<tr>
<td>supp-timeout SECONDS</td>
<td>Number of seconds that the switch waits for the retransmission of packets by the switch to the IEEE 802.1x client.</td>
<td>1-65535 seconds</td>
</tr>
<tr>
<td>tx-period SECONDS</td>
<td>Number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request.</td>
<td>1-65535 seconds</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration
Default
None

Command Purpose
Use the dot1x timeout interface configuration command on the switch stack or on a standalone switch to set IEEE 802.1x timers. Use the no form of this command to return to the default setting.

Usage
You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

The dot1x timeout re-authperiod interface configuration command affects the behavior of the switch only if you have enabled periodic re-authentication by using the dot1x reauthentication interface configuration command.

The default value of re-authperiod is 3600 seconds.
The default value of tx-period is 30 seconds.
The default value of supp-timeout is 30 seconds.
The default value of server-timeout is 30 seconds.

Examples
The following is sample output from the dot1x timeout command:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000

Related Commands
dot1x reauthentication
dot1x guest-vlan

11.9.10 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Specify an active VLAN as an 802.1x guest VLAN.</td>
<td>2-4094</td>
</tr>
</tbody>
</table>

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:

```plaintext
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 5
Switch(config-vlan)# exit
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x guest-vlan 5
```

Related Commands

show dot1x

11.9.11 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

```plaintext
show dot1x interface IFNAME
show dot1x session brief ( ( interface IFPHYSICAL ( mac MACADDR | ) | ) )
show dot1x ( all | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Specify an interface</td>
<td>Support physical ports</td>
</tr>
<tr>
<td>MACADDR</td>
<td>Specify mac address</td>
<td>MAC Address in HHHH.HHHH.HHHH format</td>
</tr>
<tr>
<td>all</td>
<td>Display IEEE 802.1x information of all interfaces</td>
<td></td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

N/A

Examples

The following is sample output from the show dot1x command:

```plaintext
Switch# show dot1x all
DUT1# show dot1x all
```
802.1X Port-Based Authentication Enabled
========================================

802.1X info for interface eth-0-2
portEnabled : false
portControl : Auto
portMode : Port based
portStatus : Unauthorized
Mac Auth bypass : disabled
reAuthenticate : enabled
reAuthPeriod : 3600
Max user number : 255
Current session number : 0
Accept user number : 0
Reject user number : 0
Guest VLAN : N/A
Assign VLAN : N/A
QuietPeriod : 60
ReqMax : 2
TxPeriod : 30
SuppTimeout : 30
ServerTimeout : 30
CD: adminControlledDirections : in
CD: operControlledDirections : in
CD: bridgeDetected : false

Related Commands

dot1x system-auth-ctrl
dot1x port-control

11.9.12 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 | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Specify an interface</td>
<td>Support physical ports</td>
</tr>
<tr>
<td>all</td>
<td>Display IEEE 802.1x information of all interfaces</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

N/A

Examples

The following is sample output from the show dot1x command:

Switch# show dot1x statistics interface eth-0-1
802.1X statistics for interface eth-0-1
   EAPOL Frames Rx: 0 - EAPOL Frames Tx: 323
   EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0
   EAP Rsp/Id Frames Rx: 0 - EAP Response Frames Rx: 0
   EAP Req/Id Frames Tx: 241 - EAP Request Frames Tx: 0
   Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
   EAPOL Last Frame Version Rx: 0 - EAPOL Last Frame Src: 0000.0000.0000

Related Commands
dot1x system-auth-ctrl
dot1x port-control
11.9.13 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
ddebug dot1x (event | timer | packet | all )
ndebug dot1x (event | timer | packet | all )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>event</td>
<td>put out the debug message of dot1x events</td>
<td>-</td>
</tr>
<tr>
<td>timer</td>
<td>put out the debug message of dot1x timer information</td>
<td>-</td>
</tr>
<tr>
<td>packet</td>
<td>put out the debug message of dot1x packets information, include sent and received</td>
<td>-</td>
</tr>
<tr>
<td>all</td>
<td>put out all debug message mentioned above</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
Use command "terminal monitor" to make debug messages print on the VTY immediately.
Use command "show logging buffer" to check the debug messages in the logging buffer.

Examples
The following is sample to open dot1x debug switches:

Switch# debug dot1x all

Related Commands
terminal monitor
show logging buffer
11.9.14 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 | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Display IEEE 802.1x information of all interfaces</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
Use the command “clear dot1x” to clear the IEEE 802.1x statistics for the switch or for the specified port.
Use the command “show dot1x” to display the IEEE 802.1x statistics.

Examples
The following is sample to using the clear dot1x command:
```
Switch# clear dot1x statistics
Switch# clear dot1x session-statistics
```

Related Commands
dot1x system-auth-ctrl
dot1x port-control
show dot1x

11.9.15 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>port</td>
<td>Set dot1x port based</td>
<td>-</td>
</tr>
<tr>
<td>mac</td>
<td>Set dot1x mac based</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration
**Default**

By default the mode is port based.

**Usage**

Use the "dot1x port-mode" command to set control mode of the interface.

Use the no form of this command to restore the default value.

dot1x port-control must be enabled before set the control mode.

The control mode cannot be changed if there are users on line.

**Examples**

The following is a sample to use the dot1x port-mode command:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dot1x port-mode mac
```

**Related Commands**

dot1x port-control

**11.9.16 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>COUNT</td>
<td>Max user number of the port</td>
<td>1-255</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

By default the user number is uncontrolled on port. The max number is according to the system hardware profile.

**Usage**

Use the "dot1x max-user" command to set max user of the interface.

Use the no form of this command to restore the default value.

dot1x port-control must be enabled before set the max value.

If there are users online, the set value should be larger than or at least be same as the users count.

The set value cannot be larger than the hardware resource count.

This count should limit the number of dot1x mac based user in state “accept”, “reject” and “reauth”, which should use hardware table for forwarding or discarding. The total number of users include “waiting” states should be 2 times as this configuration.

**Examples**

The following is a sample to use the dot1x max-user command:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dot1x max-user 10

Related Commands
dot1x port-control

11.9.17 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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>host HOST_IP_ADDR</td>
<td>Re-active the radius-server by server ip</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PORT</td>
<td>Re-active the radius-server by server ip and udp port. If the auth port is not specified the default port is 1812.</td>
<td>1-65535</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Re-active the radius-servers by IEEE 802.1x client's interface</td>
<td>This function supports routed port and access port, and Does not Support trunk port</td>
</tr>
<tr>
<td>all</td>
<td>Re-active all radius-servers</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
Use this command to active the radius server. Users do not need the wait for the radius-server dead time with this command.

Examples
The following is samples to use the dot1x re-active radius-server command:

Switch# dot1x re-activate radius-server
Switch# dot1x re-activate radius-server host 3.3.3.3 auth-port 1812
Switch# dot1x re-activate radius-server interface eth-0-9

Related Commands
radius-server host
radius-server deadtime
show radius-server
11.10 Arp Inspection Commands

11.10.1 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
Dest Mac Validation : Disabled
IP Address Validation : Disabled
Vlan Configuration : Static ACL
=================================================================
1 enabled acl
Vlan ACL Logging DHCP Logging
=================================================================
1 deny deny deny
Vlan DHCP Permits ACL Permits Source MAC Failures
=================================================================
1 0 0 0
Vlan Dest MAC Failures IP Validation Failures Invalid Protocol Data
=================================================================
1 0 0 0
```

Related Commands
ip arp inspection vlan

11.10.2 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)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical/aggregation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trust State</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-0-1</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-2</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-3</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-4</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-5</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-6</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-7</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-8</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-9</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-10</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-11</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-12</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-13</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-14</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-15</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-16</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-17</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-18</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-19</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-20</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-21</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-22</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-23</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-24</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-25</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-26</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-27</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-28</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-29</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-30</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-31</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-32</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-33</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-34</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-35</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-36</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-37</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-38</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-39</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-40</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-41</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-42</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-43</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-44</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-45</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-46</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-47</td>
<td>untrusted</td>
</tr>
<tr>
<td>eth-0-48</td>
<td>untrusted</td>
</tr>
</tbody>
</table>
Related Commands
ip arp inspection trust

11.10.3 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 | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>Specify the number of message</td>
<td>1-1024</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
No default is defined.

Usage
This command is used to verify arp inspection log settings.

Examples
This example shows how to display the log information in arp inspection log buffer:

Switch# show ip arp inspection log

Total Log Buffer Size: 32
Syslog rate: 5 entries per 1 seconds.
No entries in log buffer

Related Commands
ip arp inspection log-buffer

11.10.4 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 | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan VLAN_RNG_STR</td>
<td>Selected vlan range</td>
<td>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</td>
</tr>
</tbody>
</table>
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
```

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Forwarded</th>
<th>Dropped</th>
<th>DHCP Drops</th>
<th>ACL Drops</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vlan</th>
<th>DHCP Permits</th>
<th>ACL Permits</th>
<th>Source MAC Failures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Dest MAC Failures</th>
<th>IP Validation Failures</th>
<th>Invalid Protocol Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Related Commands
clear ip arp inspection statistics

11.10.5 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan VLAN_RNG_STR</td>
<td>Selected vlan range</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Configuration</th>
<th>ACL Match</th>
<th>Static ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enabled</td>
<td>acl</td>
<td></td>
</tr>
</tbody>
</table>

Source Mac Validation : Disabled
Destination Mac Validation : Disabled
IP Address Validation : Disabled
Vlan Configuration ACL Match Static ACL
=================================================================
1 enabled acl
Vlan ACL Logging DHCP Logging
=================================================================
1 deny deny

Related Commands

ip arp inspection vlan

11.10.6 show debugging arp inspection

Command Purpose
Use this command to display the debug information of ARP Inspection.

Command Syntax
show debugging arp inspection

Command Mode
Privileged EXEC

Default
No default is defined.

Usage
This command is used to show the general configuration of arp inspection.

Examples
This example shows how to display the debug information of ARP Inspection:

Switch# show debugging arp inspection
arp inspection debugging status:
packet debugging is on
error debugging is on

Related Commands

debug arp inspection

11.10.7 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 )
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>acl</td>
<td>ARP acl name</td>
<td>-</td>
</tr>
<tr>
<td>VLAN_rng_str</td>
<td>Selected vlan range</td>
<td>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</td>
</tr>
<tr>
<td>static</td>
<td>Apply the ACL statically</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
No default is defined.

**Usage**
This command is used to show the general configuration of arp inspection.

**Examples**
This example shows how to apply the ARP ACL to a vlan 2:

```
Switch# configure terminal
Switch(config)# ip arp inspection filter acl vlan 2 static
```

**Related Commands**
arp access-list

**11.10.8 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>Number of log buffer</td>
<td>10-1024</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
None

**Usage**
The no command reverts the log-buffer to the default buffer size (32).
Examples
This example shows how to set log-buffer size to 10:

```
Switch# configure terminal
Switch(config)# ip arp inspection log-buffer entries 10
```

Related Commands
show ip arp inspection log

11.10.9 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>Number of log buffer</td>
<td>0-1024</td>
</tr>
<tr>
<td>INTERVAL</td>
<td>Interval (seconds)</td>
<td>0-86400 seconds</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
Default number of log buffer is 5, default interval is 1

Usage
A 0 value for the logs number indicates that the entries should not be logged out of this buffer. The default number is 5.
A 0 value for the interval seconds keyword and argument indicates an immediate log. The default number is 1.

Examples
This example shows how to configure logging to send 12 messages every 2 seconds:

```
Switch# configure terminal
Switch(config)# ip arp inspection log-buffer logs 12 interval 2
```

Related Commands
None

11.10.10 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 )
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dst-mac</td>
<td>Validate destination MAC address</td>
<td>-</td>
</tr>
<tr>
<td>ip</td>
<td>Validate IP addresses</td>
<td>-</td>
</tr>
<tr>
<td>src-mac</td>
<td>Validate source MAC address</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

No default is defined.

**Usage**

For src-mac, check the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

For dst-mac, check the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

For ip, check the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.

**Examples**

This example shows how to enable additional validation on the destination MAC address:

Switch# configure terminal
Switch(config)# ip arp inspection validate dst-mac

**Related Commands**

show ip arp inspection

**11.10.11 ip arp inspection vlan**

**Command Purpose**

Use this command to enable ARP Inspection on vlans.

**Command Syntax**

[ no ] ip arp inspection vlan VLAN_ID

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan range</td>
<td></td>
</tr>
</tbody>
</table>

Valid vlan ID range is 1-4094. Use short bar(\(\)) to describe continuous VLANS, use comma(,) to describe non-continuous VLANS. For example: 1, 3-5, 7, 9-11

**Command Mode**

Global Configuration

**Default**

No default is defined.
Usage

Enable ARP Inspection on vlans.

Examples

This example shows how to enable ARP Inspection on VLAN 2:

Switch# configure terminal
Switch(config)# ip arp inspection vlan 2

Related Commands

show ip arp inspection vlan 2

11.10.12 ip arp inspection vlan logging acl-match

Command Purpose

Use this command to configure ARP Inspection log filtering.

Command Syntax

[ no ] ip arp inspection vlan VLAN_ID logging acl-match ( matchlog | none )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan range</td>
<td>Vlan range</td>
</tr>
<tr>
<td></td>
<td>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</td>
<td></td>
</tr>
</tbody>
</table>

matchlog Log packets on ACE logging configuration

none Do not log packets that match ACLs

Command Mode

Global Configuration

Default

No default is defined.

Usage

If you specify the matchlog keyword in this command and the log keyword in the permit or deny ARP access-list configuration command, ARP packets permitted or denied by the ARP Inspection are logged.

Examples

This example shows how to log permitted ARP packets on vlan 2:

Switch# configure terminal
Switch(config)# ip arp inspection vlan 2 logging acl-match matchlog

Related Commands

ip arp inspection vlan
11.10.13  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 }
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan range</td>
<td>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</td>
</tr>
<tr>
<td>all</td>
<td>Log all packets that match DHCP bindings</td>
<td>-</td>
</tr>
<tr>
<td>permit</td>
<td>Log DHCP Binding Permitted packets</td>
<td>-</td>
</tr>
<tr>
<td>none</td>
<td>Do not log packets that match DHCP bindings</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

No default is defined.

**Usage**

If the command is set, the information that match the dhcp-bindings 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

11.10.14  clear ip arp inspection log-buffer

**Command Purpose**

Use this command to delete all log in log-buffer.

**Command Syntax**

clear ip arp inspection log-buffer

**Command Mode**

Privileged EXEC
Default
No default is defined.

Usage
This command is used to delete all log in log-buffer.

Examples
This example shows how to delete all log in log-buffer:

Switch# clear ip arp inspection log-buffer

Related Commands
ip arp inspection log-buffer logs

11.10.15 clear ip arp inspection statistics

Command Purpose
Use this command to delete all statistics of ARP Inspection.

Command Syntax
clear ip arp inspection statistics

Command Mode
Global Configuration

Default
No default is defined.

Usage
This command is used to delete all statistics of ARP Inspection.

Examples
This example shows how to delete all statistics of ARP Inspection:

Switch(config)# clear ip arp inspection statistics

Related Commands
show ip arp inspection statistics

11.10.16 ip arp inspection trust

Command Purpose
Use this command to configure the ARP Inspection interface trust state.

Command Syntax
ip arp inspection trust
no ip arp inspection trust

Command Mode
Interface Configuration
Default
No default is defined.

Usage
In a typical network configuration, you configure all switch ports connected to host ports as untrusted and configure all switch ports connected to switches as trusted.

Examples
This example shows how to configure the ARP Inspection interface eth-0-2 untrusted state:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ip arp inspection trust

Related Commands
show ip arp inspection interfaces

11.10.17 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL_NAME</td>
<td>A arp access-list name</td>
<td>String with up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
No default is defined.

Usage
In non-DHCP environments, dynamic ARP inspection can validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured IP addresses.

Examples
This example shows how to configure a ARP ACL:

Switch# configure terminal
Switch(config)# arp access-list acl1

Related Commands
show access-list arp

11.10.18 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 |)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Specify packets to reject</td>
<td>-</td>
</tr>
<tr>
<td>permit</td>
<td>Log all packets that match DHCP bindings</td>
<td>-</td>
</tr>
<tr>
<td>request</td>
<td>Log DHCP Binding Permitted packets</td>
<td>-</td>
</tr>
<tr>
<td>response</td>
<td>Do not log packets that match DHCP bindings</td>
<td>-</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>Sender address</td>
<td>IPv4 address</td>
</tr>
<tr>
<td>IP_ADDR_MASK</td>
<td>Sender wildcard bits</td>
<td>IPv4 wildcard</td>
</tr>
<tr>
<td>any</td>
<td>Any sender host</td>
<td>-</td>
</tr>
<tr>
<td>host</td>
<td>A single Sender host</td>
<td>-</td>
</tr>
<tr>
<td>MAC_ADDR</td>
<td>Sender host's MAC address</td>
<td>MAC address in HHHH.HHHH.HHHH format</td>
</tr>
<tr>
<td>MAC_ADDR_MASK</td>
<td>Sender wildcard</td>
<td>MAC wildcard in HHHH.HHHH.HHHH format</td>
</tr>
<tr>
<td>log</td>
<td>Log at match</td>
<td>-</td>
</tr>
</tbody>
</table>

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-ac1)# permit ip host 192.168.1.1 mac any
```

Related Commands

show access-list arp

11.10.19 no sequence-num

Command Purpose

Use this command to delete a ARP ACE.

Command Syntax

```
no sequence-num NUMBER
```
### Command Mode
ARP ACL Configuration

### Default
No default is defined.

### Usage
This command is used to delete ARP ACE configured.

### Examples
This example shows how to delete a ARP ACE:

```
Switch# configure terminal
Switch(config)# arp access-list acl1
Switch(config-arp-acl)# no sequence-num 10
```

### Related Commands
- `show access-list arp`
- `11.10.20 show access-list arp`

### Command Purpose
Use this command to display the arp acl configuration.

### Command Syntax
```
show access-list arp (ACL_NAME | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL_NAME</td>
<td>A arp access-list name</td>
<td>String with up to 40 characters</td>
</tr>
</tbody>
</table>

### Command Mode
Privileged EXEC

### Default
No default is defined.

### Usage
This command is used to display the arp acl configured by arp acl.

### Examples
This example shows how to display arp ace:

```
Switch# show access-list arp
arp access-list acl
  10 permit request ip 1.1.1.1 0.255.255.255 mac any
```

### Related Commands
- `arp access-list`
11.11 DHCP Snooping Commands

11.11.1 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 )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>bindings</td>
<td>Clear the DHCP snooping binding database</td>
<td>-</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>Clear the binding entry by IP address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>MAC_ADDR</td>
<td>Clear the binding entry by MAC address</td>
<td>MAC Address</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>Clear the binding entry by VLAN</td>
<td>1-4094</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Clear the binding entry by interface</td>
<td>Support physical and AGG interfaces</td>
</tr>
<tr>
<td>statistics</td>
<td>Clear the DHCP snooping statistics counter</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
No default is defined.

Usage
This command is used to clear DHCP snooping binding or statistics.

Examples
This example shows how to clear the DHCP snooping statistics counters:

```
Switch(config)# clear dhcp snooping statistics
```

Related Commands
show dhcp snooping binding
show dhcp snooping statistics

11.11.2 dhcp snooping

Command Purpose
Use the dhcp snooping global configuration command on the switch to globally enable DHCP snooping. Use the no form of this command to return to the default setting.
Command Syntax

dhcp snooping

no dhcp snooping

Command Mode

Global Configuration

Default

DHCP snooping is disabled.

Usage

For any DHCP snooping configuration to take effect, you must globally enable DHCP snooping. DHCP snooping is not active until you enable snooping on a VLAN by using the dhcp snooping vlan vlan-id global configuration command.

Examples

This example shows how to enable DHCP snooping:

Switch# configure terminal
Switch(config)# dhcp snooping

You can verify your settings by entering the show dhcp snooping config privileged EXEC command:

Related Commands

dhcp snooping vlan

show dhcp snooping config

11.11.3  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 | )
### Command Mode

Global Configuration

### Default

No default database is defined.

### Usage

Use this command when you are testing or debugging the switch.

In the DHCP snooping binding database, each database entry, also referred to a binding, has an IP address, an associated MAC address, the lease time, the interface to which the binding applies, and the VLAN to which the interface belongs.

Use the show dhcp snooping binding privileged EXEC command to display the configured bindings.

### Examples

This example shows how to generate a DHCP binding configuration with an expiration time of 1000 seconds on a port in VLAN 1:

```
Switch# configure terminal
Switch(config)# dhcp snooping binding mac 0001.000c.01ef vlan 1 ipv4 10.10.1.1 interface eth-0-1 expiry 1000
```

### Related Commands

dhcp snooping

show dhcp snooping binding

### 11.11.4 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>interval SECONDS</td>
<td>Specify the interval (in seconds) that how long to save the binding database.</td>
<td>15 - 1200 seconds</td>
</tr>
</tbody>
</table>
**Command Mode**

Global Configuration

**Default**

Default interval is 600 seconds.

**Usage**

The DHCP snooping database is saved as flash:/dhcpsnooping.

**Examples**

The following is sample output from the dhcp snooping database command:

```
Switch# configure terminal
Switch(config)# dhcp snooping database auto-save interval 120
```

**Related Commands**

dhcp snooping
dhcp snooping binding

### 11.11.5 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 the reply to the switch if the request has been relayed to the server by the switch. When the client and server are on the same subnet, the server broadcasts the reply. The switch inspects the remote ID and possibly the circuit ID fields to verify that it originally inserted the option-82 data. The switch removes the option-82 field and forwards the packet to the switch port that connects to the DHCP host that sent the DHCP request.

**Examples**

This example shows how to enable DHCP option-82 data insertion:
Switch# configure terminal
Switch(config)# dhcp snooping information option

You can verify your settings by entering the show dhcp snooping config privileged EXEC command:

Switch# show dhcp snooping config
dhcp snooping service: enabled
dhcp snooping switch: enabled
Verification of hwaddr field: enabled
Insertion of relay agent information (option 82): enabled
Relay agent information (option 82) on untrusted port: not allowed
dhcp snooping vlan 1

Related Commands
show dhcp snooping config
show dhcp snooping binding

11.11.6 dhcp snooping information option allow-untrusted

Command Purpose
Use the dhcp snooping information option allow-untrusted global configuration command on an aggregation switch to configure it to accept DHCP packets with option-82 information that are received on untrusted ports that might be connected to an edge switch. Use the no form of this command to return to the default setting.

Command Syntax
dhcp snooping information option allow-untrusted
no dhcp snooping information option allow-untrusted

Command Mode
Global Configuration

Default
The switch drops DHCP packets with option-82 information that are received on untrusted ports that might be connected to an edge switch.

Usage
You might want an edge switch to which a host is connected to insert DHCP option-82 information at the edge of your network. You might also want to enable DHCP security features, such as DHCP snooping, IP source guard, or dynamic Address Resolution Protocol (ARP) inspection, on an aggregation switch. However, if DHCP snooping is enabled on the aggregation switch, the switch drops packets with option-82 information that are received on an untrusted port and does not learn DHCP snooping bindings for connected devices on a trusted interface.

If the edge switch to which a host is connected inserts option-82 information and you want to use DHCP snooping on an aggregation switch, enter the dhcp snooping information option allow-untrusted command on the aggregation switch. The aggregation switch can learn the bindings for a host even though the aggregation switch receives DHCP snooping packets on an untrusted port. You can also enable DHCP security features on the aggregation switch. The port on the edge switch to which the aggregation switch is connected must be configured as a trusted port.

Examples
This example shows how to configure an access switch to not check the option-82 information in untrusted packets from an edge switch and to accept the packets:

Switch# configure terminal
Switch(config)# dhcp snooping information option allow-untrusted

Related Commands
show dhcp snooping config
11.11.7 dhcp snooping verify

**Command Purpose**

Use the dhcp snooping verify global configuration command on the switch to configure the switch to verify on an untrusted port that the source MAC address in a DHCP packet matches the client hardware address. Use the no form of this command to configure the switch to not verify the MAC addresses.

**Command Syntax**

dhcp snooping verify mac-address

no dhcp snooping verify mac-address

**Command Mode**

Global Configuration

**Default**

The switch verifies the source MAC address in a DHCP packet that is received on untrusted ports matches the client hardware address in the packet.

**Usage**

In a service-provider network, when a switch receives a packet from a DHCP client on an untrusted port, it automatically verifies that the source MAC address and the DHCP client hardware address match. If the addresses match, the switch forwards the packet. If the addresses do not match, the switch drops the packet.

**Examples**

This example shows how to disable the MAC address verification:

```
Switch# configure terminal
Switch(config)# no dhcp snooping verify mac-address
```

**Related Commands**

show dhcp snooping config

11.11.8 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN-RANGE</td>
<td>Specify a VLAN ID or a range of VLANs on which to enable DHCP snooping.</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

DHCP snooping is disabled on all VLANs.
Usage
You can enter a single VLAN ID identified by VLAN ID number, a series of VLAN IDs separated by commas, a range of VLAN IDs separated by hyphens, or a range of VLAN IDs separated by entering the starting and ending VLAN IDs separated by a space.

You must first globally enable DHCP snooping before enabling DHCP snooping on a VLAN.

Examples
This example shows how to enable DHCP snooping on VLAN 10:

```
Switch# configure terminal
Switch(config)# dhcp snooping vlan 10
```

Related Commands
show dhcp snooping config

11.11.9 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Specify a VLAN ID.</td>
<td>1-4094</td>
</tr>
<tr>
<td>STRING</td>
<td>ASCII string for circuit id</td>
<td>ASCII string with up to 63 characters</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
None

Usage
User must globally enable DHCP snooping configuration command for any DHCP snooping configuration to take effect.

Examples
This example shows how configure the option-82 circuit-ID suboption:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dhcp snooping vlan 2 information option format-type circuit-id string vlan2
```

Related Commands
None

11.11.10 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Specify a remote ID</td>
<td>ASCII string with up to 63 characters (no spaces)</td>
</tr>
<tr>
<td>hostname</td>
<td>Specify the switch hostname as the remote ID</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

You must globally enable DHCP snooping configuration command for any DHCP snooping configuration to take effect.

Examples

This example shows how configure the option-82 remote-ID suboption:

```
Switch# configure terminal
Switch(config)# dhcp snooping information option format remote-id hostname
```

Related Commands

None

11.11.11 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

d debug dhcp snooping (events | error | dump | packet | all)

no debug dhcp snooping (events | error | dump | packet | all)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>events</td>
<td>Snooping events</td>
<td>-</td>
</tr>
<tr>
<td>error</td>
<td>Error DHCP message</td>
<td>-</td>
</tr>
<tr>
<td>packet</td>
<td>DHCP message fields</td>
<td>-</td>
</tr>
<tr>
<td>dump</td>
<td>Dump message in hex format</td>
<td>-</td>
</tr>
<tr>
<td>all</td>
<td>Turn all debugging on</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC
Default
None

Usage
Use command “terminal monitor” to make debug messages print on the VTY immediately.
Use command “show logging buffer” to check the debug messages in the logging buffer.

Examples
The following is sample to open dhcp snooping debug switches:
Switch# debug dhcp snooping all

Related Commands
terminal monitor
show logging buffer

11.11.12 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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Display all entries</td>
<td>-</td>
</tr>
<tr>
<td>manual</td>
<td>Display static entries</td>
<td>-</td>
</tr>
<tr>
<td>learning</td>
<td>Display dynamic entries</td>
<td>-</td>
</tr>
<tr>
<td>MAC_ADDR</td>
<td>Specify MAC address</td>
<td>MAC Address</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>Specify a VLAN number</td>
<td>1-4094</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>Specify an IP address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Specify an interface on which to add or delete a binding entry</td>
<td>Support physical and aggregation interfaces</td>
</tr>
<tr>
<td>summary</td>
<td>Display summary information of DHCP snooping bindings</td>
<td>-</td>
</tr>
<tr>
<td>database</td>
<td>Display stored information of DHCP snooping bindings</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
If DHCP snooping is enabled and an interface changes to the down state, the switch does not delete the statically configured bindings.
Examples

The following is sample output from the show dhcp snooping binding command:

Switch# show dhcp snooping binding all

DHCP snooping binding table:
VLAN MAC Address Interface Lease(s) IP Address
1 0001.0001.0001 eth-0-2 static 1.1.1.1

Related Commands
dhcp snooping binding

11.11.13 show dhcp snooping config

Command Purpose
Use the show dhcp snooping privileged EXEC command to display the DHCP snooping configuration.

Command Syntax
show dhcp snooping config

Command Mode
Privileged EXEC

Default
None

Usage
This command is used to display the configuration of DHCP snooping.

Examples

The following is sample output from the show dhcp snooping config command:

Switch# show dhcp snooping config
dhcp snooping service: enabled
dhcp snooping switch: enabled
Verification of hwaddr field: enabled
Insertion of relay agent information (option 82): enabled
Relay agent information (option 82) on untrusted port: not allowed
dhcp snooping vlan 1

Related Commands
dhcp snooping binding

11.11.14 show dhcp snooping statistics

Command Purpose
Use the show dhcp snooping statistics privileged EXEC command to display DHCP snooping statistics.

Command Syntax
show dhcp snooping statistics

Command Mode
Privileged EXEC
Default
None

Usage
This command is used to display the statistics of DHCP snooping.

Examples
The following is sample output from the show dhcp snooping statistics command:

```
Switch# show dhcp snooping statistics
DHCP snooping statistics:
============================================================================
DHCP packets          11257
BOOTP packets         0
Packets forwarded     10381
Packets invalid       844
Packets MAC address verify failed  354
Packets dropped       516
```

Related Commands
- clear dhcp snooping statistics

11.11.15 show dhcp snooping trusted-sources

Command Purpose
Use the show dhcp snooping trusted-sources command to display DHCP snooping trusted interfaces.

Command Syntax
```
show dhcp snooping trusted-sources
```

Command Mode
Privileged EXEC

Default
None

Usage
This command is used to display the trusted interfaces of DHCP snooping.

Examples
The following is sample output from the show dhcp snooping trusted-sources command:

```
Switch# show dhcp snooping trusted-sources
List of DHCP snooping trusted interface(s):
============================================================================
eth-0-2
```

Related Commands
- dhcp snooping trust
11.12 IP Source Guard Commands

11.12.1 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC_ADDR</td>
<td>Specify a MAC address</td>
<td>MAC Address</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>Specify a VLAN number</td>
<td>1-4094</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>Specify an IPv4 address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Specify an interface on which</td>
<td>Support physical and aggregation interfaces</td>
</tr>
<tr>
<td></td>
<td>to add or delete a binding entry</td>
<td></td>
</tr>
</tbody>
</table>

**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
do ip source binding

11.12.2 ipv6 source binding

**Command Purpose**
Use the ip source binding global configuration command on the switch to configure static IP source bindings on the switch. Use the no form of this command to delete static bindings.

**Command Syntax**

```
ip source binding mac MAC_ADDR vlan VLAN_ID ipv6 IPV6_ADDR interface IFNAME
no ip source binding mac MAC_ADDR vlan VLAN_ID ipv6 IPV6_ADDR interface IFNAME
```

www.fs.com
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC_ADDR</td>
<td>Specify a MAC address</td>
<td>MAC Address</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>Specify a VLAN number</td>
<td>1-4094</td>
</tr>
<tr>
<td>IPV6_ADDR</td>
<td>Specify an IPv6 address</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Specify an interface on which to add or delete a binding entry</td>
<td>Support physical and aggregation interfaces</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
None

**Usage**
A static IP source binding entry has an IP address, its associated MAC address, and its associated VLAN number. The same MAC and IP can only be bound in one binding entry. Duplication of MAC or IP in binding entries is not allowed.

No IP source bindings are configured by default.

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

```
Switch# configure terminal
Switch(config)# ip source binding mac 0001.1234.1234 vlan 1 ipv6 1::12:11 interface eth-0-1
```

**Related Commands**

show ip source binding

no ip source binding

11.12.3 no ip source binding entries

**Command Purpose**
Use this command to delete one or more ip source binding entries.

**Command Syntax**
no ip source binding entries
no ip source binding entries vlan VLAN_ID
no ip source binding entries interface IFNAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Specify a VLAN number</td>
<td>1-4094</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Specify an interface on which to add or delete a binding entry</td>
<td>Support physical and aggregation interfaces</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
None
Usage
If neither vlan-id nor interface-id is specified, all static ip source binding entries will be deleted.

Examples

- clear the entries of eth-0-1:
  ```
  Switch# configure terminal
  Switch(config)# no ip source binding entries interface eth-0-1
  ```

- clear the entries of vlan2:
  ```
  Switch# configure terminal
  Switch(config)# no ip source binding entries vlan 2
  ```

Related Commands

- ip source binding
- show ip source binding

11.12.4 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>Specify maximum number of bindings</td>
<td>0-30</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default
10

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

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
11.12.5 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>Check only IP address</td>
<td>-</td>
</tr>
<tr>
<td>ip-mac</td>
<td>Check IP address and MAC address</td>
<td>-</td>
</tr>
<tr>
<td>ip-vlan</td>
<td>Check IP address and VLAN</td>
<td>-</td>
</tr>
<tr>
<td>ip-mac-vlan</td>
<td>Check IP address, MAC address, and VLAN</td>
<td>-</td>
</tr>
</tbody>
</table>

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

11.12.6 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 |)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Display IP source bindings for a specified interface</td>
<td>-</td>
</tr>
</tbody>
</table>
**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

### 11.13 AAA Commands

#### 11.13.1 aaa new-model

**Command Purpose**

Use this command to enable the authentication, authorization, accounting (AAA) access control model.

Use the no form of this command to disable AAA model.

**Command Syntax**

aaa new-model

no aaa new-model

**Command Mode**

Global Configuration

**Default**

None

**Usage**

Enables the AAA access control model

**Examples**

The following example shows how to enable AAA access control model:

```
Switch# configure terminal
Switch(config)# aaa new-model
```
Related Commands

show aaa status

11.13.2 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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Default method list</td>
<td>-</td>
</tr>
<tr>
<td>LISTNAME</td>
<td>An authentication list with</td>
<td>String with up to 31 characters</td>
</tr>
<tr>
<td></td>
<td>this name</td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enable password</td>
<td>-</td>
</tr>
<tr>
<td>line</td>
<td>Line password</td>
<td>-</td>
</tr>
<tr>
<td>none</td>
<td>No authentication</td>
<td>-</td>
</tr>
<tr>
<td>radius</td>
<td>RADIUS server</td>
<td>-</td>
</tr>
<tr>
<td>local</td>
<td>Local username</td>
<td>-</td>
</tr>
<tr>
<td>tacacs-plus</td>
<td>TACACS+</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

Use the aaa authentication login global configuration command to specify one or more AAA methods for use on ports running IEEE 802.1x.

Examples

The following example shows how to set authentication at login:

Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication login default local radius none

Related Commands

show aaa method-lists authentication

11.13.3 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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Default method list</td>
<td>-</td>
</tr>
<tr>
<td>LISTNAME</td>
<td>An authentication list with this name</td>
<td>String with up to 31 characters</td>
</tr>
<tr>
<td>none</td>
<td>No authentication</td>
<td>-</td>
</tr>
<tr>
<td>radius</td>
<td>RADIUS server</td>
<td>-</td>
</tr>
<tr>
<td>local</td>
<td>Local username</td>
<td>-</td>
</tr>
<tr>
<td>tacacs-plus</td>
<td>TACACS+</td>
<td>-</td>
</tr>
</tbody>
</table>

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

11.13.4 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 Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Default method list</td>
<td>-</td>
</tr>
<tr>
<td>LISTNAME</td>
<td>An accounting list with this name</td>
<td>String with up to 31 characters</td>
</tr>
<tr>
<td>start-stop</td>
<td>Send exec accounting start and stop request while logging in switch</td>
<td>-</td>
</tr>
<tr>
<td>stop-only</td>
<td>Only send exec accounting stop request while exit switch</td>
<td>-</td>
</tr>
<tr>
<td>none</td>
<td>No accounting</td>
<td>-</td>
</tr>
<tr>
<td>radius</td>
<td>RADIUS server</td>
<td>-</td>
</tr>
<tr>
<td>tacacs-plus</td>
<td>TACACS+</td>
<td>-</td>
</tr>
</tbody>
</table>

### 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

11.13.5 `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 Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Default method list</td>
<td>-</td>
</tr>
<tr>
<td>LISTNAME</td>
<td>An accounting list with this name</td>
<td>String with up to 32 characters</td>
</tr>
<tr>
<td>none</td>
<td>No accounting</td>
<td>-</td>
</tr>
<tr>
<td>tacacs-plus</td>
<td>TACACS+</td>
<td>-</td>
</tr>
</tbody>
</table>
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
11.13.6 `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`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LEVEL1</td>
<td>The max server privilege mapping to switch level 1, default 0</td>
<td>0-12</td>
</tr>
<tr>
<td>LEVEL2</td>
<td>The max server privilege mapping to switch level 2, default 1</td>
<td>1-13</td>
</tr>
<tr>
<td>LEVEL3</td>
<td>The max server privilege mapping to switch level 3, default 10</td>
<td>2-14</td>
</tr>
</tbody>
</table>

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

11.13.7 login authentication

Command Purpose

Enable authentication, authorization, accounting (AAA) authentication for logins.

Command Syntax

login authentication (default | LISTNAME)

no login authentication

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Default method list</td>
<td>-</td>
</tr>
<tr>
<td>LISTNAME</td>
<td>An authentication list with this name</td>
<td>String with up to 31 characters</td>
</tr>
</tbody>
</table>

Command Mode

Line Configuration

Default

None

Usage

None

Examples

The following example shows how to enable authentication for logins:

Switch# configure terminal
Switch(config)# line vty 0 7
Switch(config-line)# login authentication default

Related Commands

show aaa method-lists authentication

11.13.8 authorization exec

Command Purpose

Enable authentication, authorization, accounting (AAA) authorization for logins.

Command Syntax

authorization exec (default | LISTNAME)

no authorization exec
### Parameter Description Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Default method list</td>
<td>-</td>
</tr>
<tr>
<td>LISTNAME</td>
<td>An authorization list with this name</td>
<td>String with up to 31 characters</td>
</tr>
</tbody>
</table>

#### 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
11.13.9 accounting exec

#### Command Purpose
Enable authentication, authorization, accounting (AAA) accounting for logins.

#### Command Syntax
```
accounting exec (default | LISTNAME )
```

```
no accounting exec
```

### Parameter Description Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Default method list</td>
<td>-</td>
</tr>
<tr>
<td>LISTNAME</td>
<td>An accounting list with this name</td>
<td>String with up to 31 characters</td>
</tr>
</tbody>
</table>

#### 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

11.13.10 accounting commands

Command Purpose
Enable authentication, authorization, accounting (AAA) accounting for logins.

Command Syntax
accounting commands ( default | LISTNAME )

no accounting commands

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Default method list</td>
<td>-</td>
</tr>
<tr>
<td>LISTNAME</td>
<td>An accounting list with this name</td>
<td>String with up to 31 characters</td>
</tr>
</tbody>
</table>

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

11.13.11 show aaa method-lists authentication

Command Purpose
Use this command to show authentication, authorization, accounting (AAA) authentication method lists.

Command Syntax
show aaa method-lists authentication

Command Mode
Privileged EXEC

Default
None
Usage
This command is used to show authentication, authorization, accounting (AAA) authentication method lists.

Examples
The following example shows how to show authentication method lists:

Switch# show aaa method-lists authentication

```
authen queue = AAA_ML_AUTHEN_LOGIN
    name = default    state = ALIVE: radius
authen queue = AAA_ML_AUTHEN_LOGIN
    name = group_a    state = ALIVE: radius local line enable none
authen queue = AAA_ML_AUTHEN_LOGIN
    name = group_b    state = ALIVE: local line none
```

Related Commands
aaa authentication login

11.13.12 show aaa status

Command Purpose
Use this command to show authentication, authorization, accounting (AAA) status.

Command Syntax
show aaa status

Command Mode
Privileged EXEC

Default
None

Usage
This command is used to show authentication, authorization, accounting (AAA) status.

Examples
The following example shows how to show authentication, authorization, accounting status:

Switch# show aaa status

```
aaa stats:
    Authentication enable
```

Related Commands
aaa new-model

11.13.13 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

<table>
<thead>
<tr>
<th>Server</th>
<th>Switch</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>2~10</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>11~15</td>
<td>4</td>
<td>15</td>
</tr>
</tbody>
</table>
```

Related Commands
aaa privilege mapping

11.14 RADIUS Authentication Commands

11.14.1 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MINUTES</td>
<td>Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests</td>
<td>1-20 minutes</td>
</tr>
</tbody>
</table>

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”.

www.fs.com
The default value of the radius deadtime is 5 minutes.

**Examples**

The following is sample output from the radius deadtime command:

```
Switch# configure terminal
Switch(config)# radius deadtime 10
```

**Related Commands**

radius-server host

### 11.14.2 radius-server host

**Command Purpose**

To specify a RADIUS server host, use the radius-server host command in global configuration mode. To delete the specified RADIUS host, use the no form of this command.

**Command Syntax**

```
radius-server host HOST_IP_ADDR (source-interface IFNAME | source-ip SRC_IP_ADDR)
radius-server host HOST_IP_ADDR (key (8 | secret | ) STRING | retransmit RETRIES | timeout SEC | mgmt-if IPV4_ADDR auth-port AUTH_PORT) (source-interface IFNAME | source-ip SRC_IP_ADDR)
radius-server host mgmt-if IPV4_ADDR
radius-server host mgmt-if IPV4_ADDR (key (8 | secret | ) STRING | retransmit RETRIES | timeout SEC | mgmt-if IPV4_ADDR auth-port AUTH_PORT)
```

**no radius-server host (mgmt-if | ) IPV4_ADDR (mgmt-if IPV4_ADDR auth-port AUTH_PORT)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt-if</td>
<td>Management port</td>
<td>-</td>
</tr>
<tr>
<td>IPV4_ADDR</td>
<td>IPv4 address of the RADIUS server host</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IPV6_ADDR</td>
<td>IPv6 address of the RADIUS server host</td>
<td>-</td>
</tr>
<tr>
<td>AUTH_PORT</td>
<td>(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</td>
<td>1-65535</td>
</tr>
<tr>
<td>SECONDS</td>
<td>(Optional) Specifies the time out value. If no timeout value is specified, the global value is used. The default value should be 5</td>
<td>1-1000 seconds</td>
</tr>
<tr>
<td>RETRIES</td>
<td>(Optional) Specifies the retransmit value. If no retransmit value is specified, the global value is used. The default value should be 3</td>
<td>1-100</td>
</tr>
<tr>
<td>Parameter</td>
<td>Parameter Description</td>
<td>Parameter Value</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>STRING</td>
<td>(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</td>
<td>Up to 256 characters</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Name of source interface</td>
<td>Support physical/aggregation /loopback/vlan/tunnel ports</td>
</tr>
<tr>
<td>SRC_IP_ADDR</td>
<td>Source IP address</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
You can use multiple radius-server host commands to specify multiple hosts. The software searches for hosts in the order in which you specify them.

If no host-specific timeout, retransmit, or key values are specified, the global values apply to each host.

If the source interface or source IP address is specified, the packet transmit will use the related IP address as source address.

Examples
The following is sample output from the radius-server host command:

Switch# configure terminal
Switch(config)# radius-server host 10.10.1.1 key abcde

Related Commands
radius-server key
radius-server timeout

11.14.3 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RETRIES</td>
<td>Maximum number of retransmission attempts. The default is 3</td>
<td>1-100</td>
</tr>
</tbody>
</table>
**Command Mode**

Global Configuration

**Default**

3 attempts

**Usage**

The switch tries all servers, allowing each one to time out before increasing the retransmit count.

If the RADIUS server is only a few hops from the switch, we recommend that you configure the RADIUS server retransmit rate to 5.

The default value of radius retransmit is 3 attempts.

**Examples**

The following is sample output from the radius retransmit command:

```
Switch# configure terminal
Switch(config)# radius retransmit 5
```

**Related Commands**

radius-server host
radius-server key

11.14.4 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>Number that specifies the timeout interval, In seconds. The default is 5 seconds.</td>
<td>1-1000 seconds</td>
</tr>
</tbody>
</table>

**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 timeout 15
```
Related Commands
radius-server host
radius-server key

11.14.5  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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEY_STRING</td>
<td>RADIUS server key-string</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
Use this command to set the shared encryption key in a switch.

Shared encryption key is the foundation of communicate between switch and server. You need set a same shared encryption string in authentication server and switch.

Examples
The following is sample output from the radius-server key command:

Switch# configure terminal
Switch(config)# radius-server key simple-key

Related Commands
radius-server host

11.14.6  show dot1x radius-server status

Command Purpose
Use the "show radius-server" command to display radius server states of each IEEE 802.1x session.

Command Syntax
show dot1x radius-server status ( interface IFNAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Specify an interface to show</td>
<td>Support Physical ports</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC
Default
None

Usage
Use this command to display the current radius-server and dead radius-servers of each IEEE 802.1 x sessions.

Examples
The following is sample output from the show radius-server command:

Switch# show dot1x radius-server status
====================================
802.1X session on interface eth-0-9:
current radius server:
retransmit count : 3
server address : 3.3.3.3:1812
socket descriptor : 15
last state : 
radius servers in dead list:
N/A
====================================

Related Commands
radius-server host
11.14.7 show radius-server

Command Purpose
Use the "show radius-server" command to display radius server states of each IEEE 802.1x session.

Command Syntax
show radius-server

Command Mode
Privileged EXEC

Default
None

Usage
Use this command to display the current radius-server and dead radius-servers of each IEEE 802.1 x sessions.

Examples
The following is sample output from the show radius-server command:

Switch# show radius-server
====================================
802.1X session on interface eth-0-9:
current radius server:
retransmit count : 3
server address : 3.3.3.3:1812
socket descriptor : 15
last state : 
radius servers in dead list:
N/A
====================================
Related Commands
radius-server host

11.15 Tacacs+ Commands

11.15.1 tacacs-server host

Command Purpose
Specifies and defines the IP address of the TACACS+ server host.

Command Syntax

tacacs-server host HOST_IP_ADDR ( ( key ( 8 | secret | ) STRING | timeout SECONDS | port PORT | single-connection ) | ) ( source-interface IFNAME | source-ip SRC_IP_ADDR )

tacacs-server host mgmt-if IP_ADDR ( ( key ( 8 | secret | ) STRING | timeout SECONDS | port PORT | single-connection ) | )

no tacacs-server host ( mgmt-if | ) IP_ADDR ( port PORT )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt-if</td>
<td>Management port</td>
<td>-</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>TACACS+ server IP address</td>
<td>IPv4 address</td>
</tr>
<tr>
<td>single-connection</td>
<td>Maintains a single open connection</td>
<td>-</td>
</tr>
<tr>
<td>PORT</td>
<td>TACACS server port number (default 49)</td>
<td>1-65535</td>
</tr>
<tr>
<td>SECONDS</td>
<td>Time to wait for a TACACS server to reply, the range is 1 to 20, default 5s</td>
<td>1-20</td>
</tr>
<tr>
<td>STRING</td>
<td>Set TACACS+ encryption key</td>
<td>Up to 256 characters</td>
</tr>
<tr>
<td>8</td>
<td>Specifies a hidden password will follow</td>
<td>-</td>
</tr>
<tr>
<td>secret</td>
<td>Display the current shared key with cipher text</td>
<td>-</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Name of source interface</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
<tr>
<td>SRC_IP_ADDR</td>
<td>Source IP address</td>
<td>IPv4 address</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
No Tacacs+ server is configured by default

Usage
Add or delete a TACACS+ server host.
If the source interface or source IP address is specified, the packet transmit will use the related IP address as source address.
Examples
The following example shows how to specify a TACACS+ server host:

Switch# configure terminal
Switch(config)# tacacs-server host 10.10.10.1 port 55 key my_key

Related Commands
show tacacs

11.15.2 clear tacacs statistics

Command Purpose
To reset statistics on TACACS+ servers, use the clear tacacs statistics EXEC command.

Command Syntax
clear tacacs statistics

Command Mode
Privileged EXEC

Default
None

Usage
Reset statistics on TACACS+ servers.

Examples
The following example shows how to reset statistics on TACACS+ servers:

Switch# clear tacacs statistics

Related Commands
show tacacs

11.15.3 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

<table>
<thead>
<tr>
<th>Tacacs+ Server</th>
<th>: 1.2.3.4/49</th>
</tr>
</thead>
<tbody>
<tr>
<td>Socket opens</td>
<td>1</td>
</tr>
<tr>
<td>Socket closes</td>
<td>0</td>
</tr>
<tr>
<td>Socket aborts</td>
<td>0</td>
</tr>
<tr>
<td>Socket errors</td>
<td>0</td>
</tr>
<tr>
<td>Socket Timeouts</td>
<td>0</td>
</tr>
<tr>
<td>Failed Connect Attempts</td>
<td>0</td>
</tr>
<tr>
<td>Total Packets Sent</td>
<td>2</td>
</tr>
<tr>
<td>Total Packets Recv</td>
<td>2</td>
</tr>
</tbody>
</table>

Related Commands

tacacs-server host

11.16 Port Isolate Commands

11.16.1 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

table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP</td>
<td>Port isolate group id</td>
<td>1-30</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

None

Usage

The ports in the same isolate-group can not communicate with each other.

The ports in different isolate-groups should not be affected by this feature.

The isolate-groups can only be configured on physical port and Link Aggregation.

Examples

The following is sample output from the port-isolate group command:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# port-isolate group 4
Related Commands

port-isolate mode

11.16.2 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Isolate bridged packets and routed packets</td>
<td>-</td>
</tr>
<tr>
<td>l2</td>
<td>Isolate bridged packets</td>
<td>-</td>
</tr>
</tbody>
</table>

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

11.16.3 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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP</td>
<td>Port isolate group id</td>
<td>1-30</td>
</tr>
</tbody>
</table>

www.fs.com
Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following is sample output from the show port-isolate command:

```
switch # show port-isolate group 12
Port Isolate Mode : L2
---
Port Isolate Groups:
---
Groups ID: 12
eth-0-1   eth-0-2   eth-0-3   eth-0-4   eth-0-5
eth-0-6
---
```

Related Commands
port-isolate group

11.17 Private Vlan Commands

11.17.1 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 )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>Set the port as private vlan, host port</td>
<td>-</td>
</tr>
<tr>
<td>promiscuous</td>
<td>Set the port as private vlan, promiscuous port</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
By default the switch port’s mode is access vlan.

Usage
To configure the switch port’s mode as private vlan, use the “switchport mode private-vlan” command in interface mode. This can only be configured on a switchport.
Examples

The following example shows how to configure the switch port mode:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport mode private-vlan promiscuous

Related Commands

switchport private-vlan

11.17.2 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 \}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>private-vlan VLAN_ID</td>
<td>Set private primary vlan</td>
<td>1-4094</td>
</tr>
<tr>
<td>isolate</td>
<td>Set as isolate mode</td>
<td>-</td>
</tr>
<tr>
<td>community-vlan VLAN_ID</td>
<td>Set community vlan</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

By default, the primary vlan is 1.

If the switchport mode is private-vlan host, the default mode is isolate; Or else the switchport mode is promiscuous

Usage

To configure the primary and secondary vlan of a private vlan, use the "switchport private-vlan" command in interface mode.

This can only be configured on a switchport.

Examples

The following example shows how to configure the private vlan:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan 1 isolate
Switch(config-if)# quit
Switch(config)# interface eth-0-2
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan 1 community-vlan 2
Switch(config-if)# quit
Switch(config)# interface eth-0-3
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan 1

Related Commands

switchport mode private-vlan
11.17.3 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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Show by primary vlan</td>
<td>1-4094</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Show by interface</td>
<td>Support physical/aggregation ports</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
N/A

Usage
N/A

Examples
The following example shows the result of this command:

Switch# show private-vlan

<table>
<thead>
<tr>
<th>Primary</th>
<th>Secondary Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>N/A</td>
<td>promiscuous eth-0-3</td>
</tr>
<tr>
<td>1</td>
<td>N/A</td>
<td>isolate eth-0-1</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>community eth-0-2</td>
</tr>
</tbody>
</table>

DUT1# show private-vlan vlan 1

<table>
<thead>
<tr>
<th>Primary</th>
<th>Secondary Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>N/A</td>
<td>promiscuous eth-0-3</td>
</tr>
<tr>
<td>1</td>
<td>N/A</td>
<td>isolate eth-0-1</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>community eth-0-2</td>
</tr>
</tbody>
</table>

DUT1# show private-vlan interface eth-0-1

Private vlan mode: isolate
Primary vlan id : 1

Related Commands
switchport mode private-vlan
switchport private-vlan

11.18 DDOS Commands

11.18.1 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>Specify max counter of received packets per second</td>
<td>0-1000</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
By default, ip icmp intercept is unset.
If the maxcount is not specified, the default count is 500.

Usage
Use this command if you want to set the system to limit the ICMP packet rate.

Examples
The following example shows how to configure the ip icmp intercept:

Switch# configure terminal
Switch(config)# ip icmp intercept maxcount 100

The following example unset the ip icmp intercept:

Switch# configure terminal
Switch(config)# no ip icmp intercept

Related Commands
show ip-intercept config

11.18.2 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

11.18.3 ip fraggle intercept

Command Purpose

To configure the system to resist fraggle attack, use the ip fraggle intercept command in global configuration mode. To disable this capability, use the no form of this command.

Command Syntax

```
ip fraggle intercept
no ip fraggle intercept
```

Command Mode

Global Configuration

Default

By default, ip fraggle intercept is unset.

Usage

Use this command if you want to set the system to resist fraggle attack.

Examples

The following example shows how to configure the ip fraggle intercept:

```
Switch# configure terminal
Switch(config)# ip fraggle intercept
```

The following example unset the ip fraggle intercept:

```
Switch# configure terminal
Switch(config)# no ip fraggle intercept
```

Related Commands

show ip-intercept config

11.18.4 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
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>Specify max counter of received packets per second</td>
<td>0-1000</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
By default, ip udp intercept is unset.
If the maxcount is not specified, the default count is 500.

**Usage**
Use this command if you want to set the system to limit the UDP packet rate.

**Examples**
The following example shows how to configure the ip udp intercept:

```
Switch# configure terminal
Switch(config)# ip udp intercept maxcount 100
```

The following example unset the ip udp intercept:

```
Switch# configure terminal
Switch(config)# no ip udp intercept
```

**Related Commands**
show ip-intercept config

**11.18.5 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>Specify max counter of received packets per second</td>
<td>0-1000</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
By default, ip tcp intercept is unset.
If the maxcount is not specified, the default count is 500.

**Usage**
Use this command if you want to set the system to limit the TCP packet rate with only SYN bit set.
Examples

The following example shows how to configure the ip tcp intercept:

Switch# configure terminal
Switch(config)# ip tcp intercept maxcount 100

The following example unset the ip tcp intercept:

Switch# configure terminal
Switch(config)# no ip tcp intercept

Related Commands

show ip-intercept config

11.18.6 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>Specify length of small packet</td>
<td>28-65535</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

By default, ip small-packet intercept is unset.

If the length is not specified, the default value is 28 bytes.

Usage

Use this command if you want to set the system to drop the packet which length is less than the configured value.

Examples

The following example configures the ip small-packet intercept:

Switch# configure terminal
Switch(config)# ip small-packet intercept length 32

The following example unset the ip small-packet intercept:

Switch# configure terminal
Switch(config)# no small-packet intercept

Related Commands

show ip-intercept config

11.18.7 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 configure the ip intercept mac equals:

Switch# configure terminal
Switch(config)# ip maceq intercept

The following example unset the ip intercept mac equals:

Switch# configure terminal
Switch(config)# no ip maceq intercept

Related Commands
show ip-intercept config

11.18.8 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 configure the ip intercept ip equal:

Switch# configure terminal
Switch(config)# ip ipeq intercept

The following example unset the ip intercept ip equal:
Switch# configure terminal
Switch(config)# no ip ipeq intercept

Related Commands
show ip-intercept config

11.18.9 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:
================================================================挑战
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
Smurf Attack Intercept :Enable
Fraggle Attack Intercept :Enable
MAC Equal Intercept :Disable
IP Equal Intercept :Disable

Related Commands
show ip-intercept config

11.18.10 show ip-intercept statistics

Command Purpose
To display the statistics of the intercept packets, use the show ip-intercept statistics command in privileged Privileged EXEC.

Command Syntax
show ip-intercept statistics

Command Mode
Privileged EXEC

Default
None
Usage

Use this command to display ip intercept statistics.

Examples

The following is sample output from the show ip-intercept statistics command:

```
Switch# show ip-intercept statistics

Current DDoS Prevent statistics:
============================================================================
Resist Small-packet Attack packets number : 108
Resist ICMP Flood packets number        : 0
Resist Smurf Attack packets number      : 0
Resist SYN Flood packets number         : 0
Resist Fraggle Attack packets number    : 0
Resist UDP Flood packets number         : 0
```

Related Commands

clear ip-intercept statistics

11.18.11 clear ip-intercept statistics

Command Purpose

To clear the statistics of the intercept packets, use the clear ip-intercept statistics command in privileged Privileged EXEC.

Command Syntax

```
clear ip-intercept statistics
```

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to clear ip intercept statistics.

Examples

The following example displays how to use clear ip-intercept statistics command:

```
Switch# clear ip-intercept statistics
Switch# show ip-intercept statistics

Current DDoS Prevent statistics:
============================================================================
Resist Small-packet Attack packets number : 0
Resist ICMP Flood packets number        : 0
Resist Smurf Attack packets number      : 0
Resist SYN Flood packets number         : 0
Resist Fraggle Attack packets number    : 0
Resist UDP Flood packets number         : 0
```

Related Commands

```
show ip-intercept statistics
```
11.19 Key Chain Commands

11.19.1 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>The name of keychain</td>
<td>String with up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
No keychain is created.

Usage
Routing protocols and network management applications often use keychain to enhance security while communicating with peers. For the detail of these configurations, see relevant chapters of user guide.

Examples
The following example shows how to create a keychain:

```
Switch# configure terminal
Switch(config)# key chain test
Switch(config-keychain)#
```

Related Commands
key
key-string
show key chain

11.19.2 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEY_ID</td>
<td>key id</td>
<td>0-31</td>
</tr>
</tbody>
</table>
**Command Mode**

Key Chain Configuration

**Default**

There is no key in a keychain.

**Usage**

The key will not be used unless key string was configured.

**Examples**

The following example shows how to create a key:

```
Switch# configure terminal
Switch(config)# key chain test
Switch(config-keychain)# key 1
```

**Related Commands**

key chain
key-string
accept-lifetime
send-lifetime

**11.19.3 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LINE</strong></td>
<td>Key string</td>
<td>String with up to 255 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Key Configuration

**Default**

The key string is not be configured.

**Usage**

This command is used to configure key string for a key and then this key will be valid for ever if there is no lifetime set.

**Examples**

The following example shows how to configure key-string:

```
Switch# configure terminal
Switch(config)# key chain test
Switch(config-keychain)# key 2
Switch(config-keychain-key)# key-string ##test_keywords##
```
Related Commands
key
accept-lifetime
send-lifetime

11.19.4 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>START-TIME</td>
<td>The start of accept lifetime</td>
<td>The start of accept lifetime, its format should like &quot;HH:MM:SS &lt;1-31&gt; MONTH &lt;1993-2035&gt;&quot; or &quot;HH:MM:SS MONTH &lt;1-31&gt; &lt;1993-2035&gt;&quot; and MONTH should be First three letters of the month</td>
</tr>
<tr>
<td>EXPIRE-TIME</td>
<td>The end of accept lifetime</td>
<td>The end of accept lifetime, its format should like &quot;HH:MM:SS &lt;1-31&gt; MONTH &lt;1993-2035&gt;&quot;; &quot;HH:MM:SS MONTH &lt;1-31&gt; &lt;1993-2035&gt;&quot;; &quot;Infinite&quot; or &quot;duration &lt;1-2147483646&gt;&quot; and MONTH should be First three letters of the month</td>
</tr>
</tbody>
</table>

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 test
Switch(config-keychain)# key 2
Switch(config-keychain-key)# accept-lifetime 0:0:1 2 jan 2012 infinite
Related Commands
key
key-string

11.19.5 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>START-TIME</td>
<td>The start of send lifetime</td>
<td>The start of send lifetime, its format should like &quot;HH:MM:SS &lt;1-31&gt; MONTH &lt;1993-2035&gt;&quot; or &quot;HH:MM:SS MONTH &lt;1-31&gt; &lt;1993-2035&gt;&quot; and MONTH should be First three letters of the month</td>
</tr>
<tr>
<td>EXPIRE-TIME</td>
<td>The end of send lifetime</td>
<td>The end of send lifetime, its format should like &quot;HH:MM:SS &lt;1-31&gt; MONTH &lt;1993-2035&gt;&quot;, &quot;HH:MM:SS MONTH &lt;1-31&gt; &lt;1993-2035&gt;&quot;, &quot;Infinite&quot; or &quot;duration &lt;1-2147483646&gt;&quot; and MONTH should be First three letters of the month</td>
</tr>
</tbody>
</table>

Command Mode
Key Configuration

Default
No send lifetime is configured

Usage
This command is used to configure send lifetime for a key which will be invalid after lifetime expired.

Examples
The following example shows how to configure send-lifetime:

```
Switch# configure terminal
Switch(config)# key chain test
Switch(config-keychain)# key 2
Switch(config-keychain-key)# send-lifetime 0:0:1 2 jan 2012 infinite
```

Related Commands
key
key-string
11.19.6 show key chain

Command Purpose
To show information of keychain, use show key chain command.

Command Syntax
show key chain (WORD | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>The name of keychain</td>
<td>String with up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following example shows how to display keychain:

Switch# show key chain test
key chain test:
  key 1 -- text "key-string ##test_keywords_1##"
    accept-lifetime <00:00:01 Jan 01 2012> - <infinite>
    send-lifetime <always valid> - <always valid> [valid now]
  key 2 -- text "key-string ##test_keywords_2##"
    accept-lifetime <always valid> - <always valid> [valid now]
    send-lifetime <00:00:01 Jan 02 2012> - <infinite>

Related Commands
key chain

11.20 Port-block Commands

11.20.1 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 )

www.fs.com
### 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)`

### Command Syntax
```
show port-block (interface IFNAME |)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>IFNAME</code></td>
<td>Specify the interface</td>
<td>Support physical/aggregation ports</td>
</tr>
</tbody>
</table>

### Command Mode
Privileged EXEC
**Default**

N/A

**Usage**

If the interface is not specified, all interfaces should be displayed.

**Examples**

This example shows how to show port-block configuration in Privileged Privileged EXEC:

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

**Related Commands**

port-block (known-unicast | known-multicast | unknown-unicast | unknown-multicast | broadcast)

### 11.21 Device management security Commands

#### 11.21.1 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>access-list name</td>
<td>String with up to 40 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

No acl is specified

**Usage**

Use this command to deny specified telnet client IP.

The access-list should be created before using this command.

**Examples**

This example shows how to enable telnet acl, which deny telnet client with source IP 1.1.1.1:

```
Switch# configure terminal
Switch(config)# ip access-list telnetACL
Switch(config-ip-acl)# 10 deny tcp host 1.1.1.1 any
Switch(config-ip-acl)# exit
Switch(config)# ip telnet server acl telnetACL
```

**Related Commands**

None
11.21.2 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>access-list name</td>
<td>String with up to 40 characters</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
No acl is specified

Usage
Use this command to deny specified SSH client IP.
The access-list should be created before using this command.

Examples
This example shows how to enable SSH acl, which deny SSH client with source IP 1.1.1.1:

```
Switch# configure terminal
Switch(config)# ip access-list telnetACL
Switch(config-ip-acl)# 10 deny tcp host 1.1.1.1 any
Switch(config-ip-acl)# exit
Switch(config)# ip ssh server acl telnetACL
```

Related Commands
None
Chapter 12 IPv6 Security Commands

12.1 DHCPv6 Snooping Commands

12.1.1 clear dhcpv6 snooping bindings learning

Command Purpose

Use the clear dhcpv6 snooping bindings learning privileged EXEC command on the switch to clear the dynamic DHCPv6 binding items.

Command Syntax

```
clear dhcpv6 snooping bindings (learning | manual) (ipv6 IP-ADDRESS | mac MAC-ADDRESS | vlan VLAN-ID | interface IFNAME)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 IP-ADDRESS</td>
<td>Clear the binding entry with the IPv6 address</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>mac MAC-ADDRESS</td>
<td>Clear the binding entry with the MAC address</td>
<td>MAC address</td>
</tr>
<tr>
<td>vlan VLAN-ID</td>
<td>Clear the binding entry with the VLAN</td>
<td>1-4094</td>
</tr>
<tr>
<td>interface IFNAME</td>
<td>Clear the binding entry with the Interface</td>
<td>Support physical/aggregation ports</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

No default is defined.

Usage

This command is used to clear DHCPv6 snooping binding.

Examples

This example shows how to clear all DHCPv6 snooping binding learning items:

```
Switch# clear dhcpv6 snooping bindings learning
```

Related Commands

show dhcpv6 snooping binding
12.1.2 clear dhcpv6 snooping statistics

Command Purpose
Use the clear dhcpv6 snooping statistics privileged EXEC command on the switch to clear the DHCPv6 snooping statistics counters.

Command Syntax
clear dhcpv6 snooping statistics

Command Mode
Privileged EXEC

Default
No default is defined.

Usage
This command is used to clear DHCPv6 snooping statistics.

Examples
This example shows how to clear the DHCPv6 snooping statistics counters:
Switch# clear dhcpv6 snooping statistics

Related Commands
show dhcpv6 snooping statistics

12.1.3 dhcpv6 snooping

Command Purpose
Use the dhcpv6 snooping global configuration command on the switch to globally enable DHCPv6 snooping. Use the no form of this command to return to the default setting.

Command Syntax
dhcpv6 snooping
no dhcpv6 snooping

Command Mode
Global Configuration

Default
DHCPv6 snooping is disabled.

Usage
For any DHCPv6 snooping configuration to take effect, you must globally enable DHCPv6 snooping. DHCPv6 snooping is not active until you enable snooping on a VLAN by using the dhcpv6 snooping vlan global configuration command.
Examples
This example shows how to enable DHCPv6 snooping:

```plaintext
Switch# configure terminal
Switch(config)# dhcpv6 snooping
```

You can verify your settings by entering the show dhcpv6 snooping config privileged EXEC command:

Related Commands
- dhcpv6 snooping vlan
- show dhcpv6 snooping config

12.1.4 dhcpv6 snooping binding

Command Purpose
Use the dhcpv6 snooping binding global configuration command on the switch to configure the DHCPv6 snooping binding database and to add binding entries to the database.

Command Syntax
```
dhcpv6 snooping binding mac MAC-ADDRESS vlan VLAN-ID ipv6 IP-ADDRESS interface IFNAME expiry SECONDS
no dhcpv6 snooping bindings (ipv6 IP-ADDRESS | mac MAC-ADDRESS | vlan VLAN-ID | interface IFNAME |)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac MAC-ADDRESS</td>
<td>Specify a MAC address</td>
<td>MAC address</td>
</tr>
<tr>
<td>vlan VLAN-ID</td>
<td>Specify a VLAN number.</td>
<td>1-4094</td>
</tr>
<tr>
<td>ipv6 IP-ADDRESS</td>
<td>Specify an IPv6 address</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>interface IFNAME</td>
<td>Specify an interface on which to add or delete a binding entry</td>
<td>Support physical/aggregation ports</td>
</tr>
<tr>
<td>expiry SECONDS</td>
<td>Specify the interval (in seconds) after which the binding entry is no longer valid. The range is 0 to 86400</td>
<td>0-86400 seconds</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
No default database is defined.

Usage
Use this command when you are testing or debugging the switch.
In the DHCPv6 snooping binding database, each database entry, also referred to a binding, has an IP address, an associated MAC address, the lease time, the interface to which the binding applies, and the VLAN to which the interface belongs.

Use the show dhcpv6 snooping binding privileged EXEC command to display the configured bindings.
Examples
This example shows how to generate a DHCPv6 binding with an expiration time of 1000 seconds on a port in VLAN 1:

```plaintext
Switch# configure terminal
Switch(config)# dhcpv6 snooping binding mac 0001.000c.01ef vlan 1 ipv6 2001::1 interface eth-0-1 expiry 1000
```

Related Commands

show dhcpv6 snooping binding

12.1.5 dhcpv6 snooping database

Command Purpose

Use the dhcpv6 snooping database global configuration command on the switch to configure the DHCPv6 snooping binding database agent. Use the no form of this command to reset the write-delay value.

Command Syntax

```
dhcpv6 snooping database auto-save interval SECONDS
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>interval SECONDS</td>
<td>Specify the interval (in seconds) that how long to save the binding database.</td>
<td>15-2000 seconds</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

Default interval is 600 seconds.

Usage

The DHCPv6 snooping database is save as flash:/dhcpv6snooping.

Examples

The following is sample output from the dhcpv6 snooping database command:

```plaintext
Switch# configure terminal
Switch(config)# dhcpv6 snooping database auto-save interval 120
```

Related Commands

dhcpv6 snooping
dhcpv6 snooping binding
### 12.1.6 dhcpv6 snooping trust

**Command Purpose**

Use the dhcpv6 snooping trust interface configuration command on the switch to configure a port as trusted for DHCPv6 snooping purposes.
Use the no form of this command to return to the default setting.

**Command Syntax**

```
dhcpv6 snooping trust
no dhcpv6 snooping trust
```

**Command Mode**

Interface Configuration

**Default**

DHCPv6 snooping trust is disabled.

**Usage**

Configure as trusted ports those that are connected to a DHCPv6 server or to other switches or routers. Configure as entrusted ports those that are connected to DHCPv6 clients.

**Examples**

This example shows how to enable DHCPv6 snooping trust on a port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dhcpv6 snooping trust
```

**Related Commands**

show dhcpv6 snooping trusted-sources

### 12.1.7 dhcpv6 snooping vlan

**Command Purpose**

Use the dhcpv6 snooping vlan global configuration command on the switch to enable DHCPv6 snooping on a VLAN. Use the no form of this command to return to the default setting.
Command Syntax

dhcpv6 snooping vlan VLAN-RANGE
no dhcpv6 snooping vlan VLAN-RANGE

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN-RANGE</td>
<td>Specify a VLAN ID or a range of VLANs on which to enable DHCP snooping.</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

DHCPv6 snooping is disabled on all VLANs.

Usage

You can enter a single VLAN ID identified by VLAN ID number, a series of VLAN IDs separated by commas, a range of VLAN IDs separated by hyphens, or a range of VLAN IDs separated by entering the starting and ending VLAN IDs separated by a space.
You must first globally enable DHCPv6 snooping before enabling DHCPv6 snooping on a VLAN.

Examples

This example shows how to enable DHCPv6 snooping on VLAN 10:

Switch# configure terminal
Switch(config)# dhcpv6 snooping vlan 10

Related Commands

show dhcpv6 snooping config

12.1.8 debug dhcpv6 snooping

Command Purpose

Use this command to turn on the debug switches of dhcpv6 snooping module.
To restore the default, use the no form of this command

Command Syntax

d debug dhcpv6 snooping ( events | error | dump | packet | all )
no debug dhcpv6 snooping ( events | error | dump | packet | all )
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>events</td>
<td>Snooping events</td>
<td>-</td>
</tr>
<tr>
<td>error</td>
<td>Error DHCPv6 message</td>
<td>-</td>
</tr>
<tr>
<td>packet</td>
<td>DHCPv6 message fields</td>
<td>-</td>
</tr>
<tr>
<td>dump</td>
<td>Dump message in hex format</td>
<td>-</td>
</tr>
<tr>
<td>all</td>
<td>Turn all debugging on</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

Use command “terminal monitor” to make debug messages print on the VTY immediately.
Use command “show logging buffer” to check the debug messages in the logging buffer.

**Examples**

The following is sample to open dhcpv6 snooping debug switches:

Switch# debug dhcpv6 snooping all

**Related Commands**

terminal monitor
show logging buffer

**12.1.9 show dhcpv6 snooping binding**

**Command Purpose**

Use the show dhcpv6 snooping binding privileged EXEC command to display the DHCPv6 snooping binding database and configuration information for all interfaces on a switch.

**Command Syntax**

```
show dhcpv6 snooping binding { ( all | manual | learning ) ( ipv4 IP-ADDRESS | mac MAC-ADDRESS | vlan VLAN-ID | interface IFNAME ) } summary | }
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Display all entries</td>
<td>-</td>
</tr>
<tr>
<td>manual</td>
<td>Display static entries</td>
<td>-</td>
</tr>
<tr>
<td>learning</td>
<td>Display dynamic entries</td>
<td>-</td>
</tr>
<tr>
<td>mac MAC-ADDRESS</td>
<td>Specify MAC address</td>
<td>MAC address</td>
</tr>
<tr>
<td>vlan VLAN-ID</td>
<td>Specify a VLAN number.</td>
<td>1-4094</td>
</tr>
<tr>
<td>ipv4 IP-ADDRESS</td>
<td>Specify an IP address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>interface IFNAME</td>
<td>Specify an interface on which to add or delete a binding entry</td>
<td>Support physical/aggregation ports</td>
</tr>
<tr>
<td>summary</td>
<td>Display summary information of DHCPv6 snooping bindings</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

If DHCPv6 snooping is enabled and an interface changes to the down state, the switch does not delete the statically configured bindings.

**Examples**

The following is sample output from the show dhcpv6 snooping binding command:

```
Switch# show dhcpv6 snooping binding all

DHCPv6 snooping binding table:
VLAN MAC Address Interface Lease(s) IPv6 Address
============================================================
1 0001.0001.0001 eth-0-2 static 1:1:1:1
```

Switch# show dhcpv6 snooping binding summary

Total 1 DHCPv6 snooping binding entries

0 learning entry, 1 configured entry

**Related Commands**

dhcpv6 snooping binding
12.1.10 show dhcpv6 snooping config

**Command Purpose**
Use the show dhcpv6 snooping privileged EXEC command to display the DHCPv6 snooping configuration.

**Command Syntax**
show dhcpv6 snooping config

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
This command is used to display the configuration of DHCPv6 snooping.

**Examples**
The following is sample output from the show dhcpv6 snooping config command:

```
Switch# show dhcpv6 snooping config

 dhcpv6 snooping service: enabled
 dhcpv6 snooping switch: enabled
 dhcpv6 snooping vlan 3
```

**Related Commands**
dhcpv6 snooping
dhcpv6 snooping vlan

12.1.11 show dhcpv6 snooping trusted-sources

**Command Purpose**
Use the show dhcpv6 snooping trusted-sources privileged EXEC command to display the DHCPv6 snooping trusted interface.

**Command Syntax**
show dhcpv6 snooping trusted-sources

**Command Mode**
Privileged EXEC

**Default**
None
Usage
This command is used to display the trusted interface of DHCPv6 snooping.

Examples
The following is sample output from the show dhcpv6 snooping trusted-sources command:

```
Switch# show dhcpv6 snooping trusted-source

List of DHCPv6 snooping trusted interface(s):
=================================================================================================
eth-0-20
```

Related Commands
dhcpv6 snooping trust

12.1.12 show dhcpv6 snooping statistics

Command Purpose
Use the show dhcpv6 snooping statistics privileged EXEC command to display DHCPv6 snooping statistics.

Command Syntax
```
show dhcpv6 snooping statistics
```

Command Mode
Privileged EXEC

Default
None

Usage
This command is used to display the statistics of DHCPv6 snooping.

Examples
The following is sample output from the show dhcpv6 snooping statistics command:

```
Switch# show dhcpv6 snooping statistics

DHCPv6 snooping statistics:
=================================================================================================
DHCPv6 packets 137
Packets forwarded 137
Packets invalid 0
Packets dropped 0
```

Related Commands
clear dhcpv6 snooping statistics
Chapter 13 Reliability Commands

13.1 BHM Commands

13.1.1 sysmon enable

Command Purpose
Use this command to enable system monitor. Use the no command to disable system monitor.

Command Syntax
sysmon enable
no sysmon enable

Command Mode
Global Configuration

Default
Sysmon is enabled by default.

Usage
None

Examples
The following example shows how to enable system monitor:

Switch# configure terminal
Switch(config)# sysmon enable

Related Commands
show sysmon

13.1.2 show sysmon

Command Purpose
Use this command to show system monitor information.

Command Syntax
show sysmon

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following example shows how to display system monitor status:

Switch# show sysmon
System monitor enable.
Related Commands

sysmon enable

13.1.3 heart-beat-monitor enable

Command Purpose

Use this command to enable heart beat monitor. Use the no command to disable heart beat monitor.

Command Syntax

heart-beat-monitor enable
no heart-beat-monitor enable

Command Mode

Global Configuration

Default

The default of heart beat monitor is enabled.

Usage

None

Examples

The following example shows how to enable heart beat monitor:

Switch# configure terminal
Switch(config)# heart-beat-monitor enable

Related Commands

show heart-beat-monitor

13.1.4 heart-beat-monitor reactivate

Command Purpose

Use this command to specify a reactivation after process crash.

Command Syntax

heart-beat-monitor reactivate ( reload system | shutdown port | warning )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>reload system</td>
<td>reload system</td>
<td>-</td>
</tr>
<tr>
<td>shutdown port</td>
<td>shutdown all port when system crash</td>
<td>-</td>
</tr>
<tr>
<td>warning</td>
<td>print warning on screen</td>
<td>-</td>
</tr>
</tbody>
</table>

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

13.1.5 show heart-beat-monitor
Command Purpose
Use this command to show heart beat monitor status.

Command Syntax

show heart-beat-monitor

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to show system monitor information:
Switch# show heart-beat-monitor
heart-beat-monitor enable.
heart-beat-monitor reactivation: restart system.

Related Commands

heart-beat-monitor enable
heart-beat-monitor reactivate

13.2 EFM Commands

13.2.1 ethernet oam enable

Command Purpose

Use this command to enable Ethernet operations, maintenance, and administration (OAM) on an interface.
Use the no form of this command to disable OAM on an interface.

Command Syntax

ethernet oam enable
no ethernet oam enable

Command Mode

Interface Configuration

Default

The default status of Ethernet OAM is disabled.
Usage
This command is used to enable the Ethernet OAM module on a port.

Examples
The following example shows how to enable Ethernet OAM:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ethernet oam enable

Related Commands
no ethernet oam enable

13.2.2 ethernet oam mode
Command Purpose
Use the command to configure Ethernet OAM mode on an interface

Command Syntax
ethernet oam mode active
ethernet oam mode passive
no ethernet oam mode

Command Mode
Interface Configuration

Default
The default Ethernet OAM mode for the DTE is passive.

Usage
This command is used to set the DTE to active mode or passive mode.

Examples
The following example shows how to set EFM mode:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ethernet oam mode active
Switch(config-if)# ethernet oam mode passive

Related Commands
None

13.2.3 ethernet oam min-rate
Command Purpose
Use this command to set the OAMPDU timer. Use the no form of the command to reset to default value.

Command Syntax
ethernet oam min-rate SECONDS
no ethernet oam min-rate

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>The number of seconds chosen for this timer.</td>
<td>1-10 seconds</td>
</tr>
</tbody>
</table>
Command Mode

Interface Configuration

Default

The default value of the OAMPDU timer is 1 second

Usage

Set the timer to emit at least one OAMPDU per second and ensure that the sublayer adheres to the maximum number of OAMPDUs per second. The minimum is 1 OAMPDU per second and the maximum is 10 OAMPDU per second

Examples

The following example shows how to set the OAMPDU timer to 1:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ethernet oam min-rate 1

Related Commands

show ethernet oam status

13.2.4 ethernet oam max-rate

Command Purpose

Use this command to set the OAMPDU maximum number of PDUs per second. Use the no form of the command to reset max-rate to the default value.

Command Syntax

ethernet oam max-rate PDUS
no ethernet oam max-rate

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDUS</td>
<td>The maximum number of PDUs per second.</td>
<td>1-10</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

The default value of the max-rate is 10 PDUs per second.

Usage

This command is to ensure that the sublayer adheres to the maximum number of OAMPDUs per second. The minimum is 1 OAMPDU per second and the maximum is 10 OAMPDUs per second.

Examples

The following example shows how to set the OAMPDU maximum number to 10 per second:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ethernet oam max-rate 10

Related Commands

show ethernet oam status
13.2.5  ethernet oam link-monitor on

Command Purpose
Use this command to turn on link monitoring on an interface. Use the no form of this command to turn link monitoring off.

Command Syntax

```
eternet oam link-monitor on
no ethernet oam link-monitor on
```

Command Mode
Interface Configuration

Default
When link monitor is supported, link monitoring is automatically turned on.

Usage
None

Examples
The following example shows how to turn on link monitoring on interface eth-0-1:
```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ethernet oam link-monitor on
```

Related Commands
show ethernet oam status

13.2.6  ethernet oam link-monitor supported

Command Purpose
Use this command to configure link monitoring on an interface. Use the no form of this command to remove support for link monitoring on an interface.

Command Syntax

```
eternet oam link-monitor supported
no ethernet oam link-monitor supported
```

Command Mode
Interface Configuration

Default
The default state of the link monitor is supported

Usage
None

Examples
The following example shows how to configure link monitoring on interface eth-0-1:
```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ethernet oam link-monitor supported
```
Related Commands
show ethernet oam status

13.2.7 ethernet oam link-monitor frame

Command Purpose
Use this command to configure the low and high threshold and the window for the frame event. If the low threshold is exceeded, an error frame link event is generated. If the high threshold is exceeded, the action defined using the command ethernet oam link-monitor high threshold action is taken.

Command Syntax
ethernet oam link-monitor frame threshold high (HIGH_THRES | none) low LOW_THRES window WINDOW
no ethernet oam link-monitor frame threshold

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIGH_THRES</td>
<td>Value of the high threshold for error frames.</td>
<td>1-65535</td>
</tr>
<tr>
<td>none</td>
<td>No high threshold value is set</td>
<td>-</td>
</tr>
<tr>
<td>low LOW_THRES</td>
<td>Value of the low threshold for error frames.</td>
<td>0-65535</td>
</tr>
<tr>
<td>window WINDOW</td>
<td>Size of frame event window, expressed in milliseconds</td>
<td>10-600</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
The default value for high threshold is none, meaning that no high threshold is configured.
The default value of low threshold is 1.
The default value for the frame event window is 100.

Usage
None

Examples
The following example shows how to configure the low and high threshold and the window for the frame event:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ethernet oam link-monitor frame threshold high 5 low 2 window 200

Related Commands
show ethernet oam status

13.2.8 ethernet oam link-monitor frame-seconds threshold

Command Purpose
Use this command to configure the low and high threshold and the window for the frame-seconds event. If the low threshold is exceeded, an error-frame-seconds link event is generated. If the high threshold is exceeded then action defined through the command ethernet oam link-monitor high threshold action will be taken.
Command Syntax

ethernet oam link-monitor frame-seconds threshold high (HIGH_THRES | none) low LOW_THRES window WINDOW
no ethernet oam link-monitor frame-seconds threshold high

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIGH_THRES</td>
<td>High threshold for the number of error frame-seconds in the range of 1~900</td>
<td>1-900</td>
</tr>
<tr>
<td>none</td>
<td>No high threshold value is set</td>
<td>-</td>
</tr>
<tr>
<td>LOW_THRES</td>
<td>Low threshold for the number of error frame-seconds 1~900</td>
<td>1-900</td>
</tr>
<tr>
<td>window WINDOW</td>
<td>Window for frame-seconds events, in milliseconds, in multiples of 100</td>
<td>100-9000</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default

The default value for high threshold is none, meaning that no high threshold is configure. The default value for the low threshold is 1. The default value of frame event window is 1000.

Usage
None

Examples
The following example shows how to configure the threshold and window for the frame-seconds event:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ethernet oam link-monitor frame-seconds threshold high 5 low 2 window 200

Related Commands
show ethernet oam status

13.2.9 ethernet oam link-monitor high threshold action

Command Purpose

Use this command to define action when high threshold is detected. Use no form of the command to reset the action.

Command Syntax

ethernet oam link-monitor high threshold action error-disable-interface
no ethernet oam link-monitor high threshold action error-disable-interface

Command Mode
Interface Configuration

Default

When high threshold is exceeded it will generate only the corresponding link event and will not trigger any interface events by default

Usage
None
Examples

The following example shows how to define action of error-disable interface when high threshold is detected:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ethernet oam link-monitor high-threshold action error-disable-interface

Related Commands

show ethernet oam status

13.2.10 ethernet oam remote-loopback

Command Purpose

Use this command to configure remote loopback on an interface. This command can be used to enable or disable remote loopback and also configure the remote loopback timeout, which is the number of seconds the DTE will wait for the remote DTE to respond to the ethernet oam remote-loopback enable command. Use the no form of this command to remove remote-loopback support from the interface.

Command Syntax

ethernet oam remote-loopback { supported | timeout SECS }
no ethernet oam remote-loopback { supported | timeout }

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>supported</td>
<td>Remote loopback can be initiated in the DTE</td>
<td>-</td>
</tr>
<tr>
<td>timeout SECS</td>
<td>The remote loopback timeout value in the range of 1~10</td>
<td>1-10 seconds</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

The default state for the remote loopback is not supported. If a timeout is not configured, the local DTE remains in remote loopback state until the remote DTE responds or the user stops remote loopback administratively. One switch supports 4 interfaces in "local Loopback" status at the same time.

Usage

None

Examples

The following example shows how to support remote-loopback on interface eth-0-1:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ethernet oam remote-loopback supported

Related Commands

show ethernet oam status

13.2.11 ethernet oam remote-loopback start

Command Purpose
Use this command to start an Ethernet OAM remote-loopback mechanism.

**Command Syntax**

```
ethernet oam remote-loopback start interface IFNAME
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Name of the interface</td>
<td>Support physical ports</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

The default state of the remote loopback function is disabled.

**Usage**

This command is used to start a remote loopback mechanism.

**Examples**

The following example shows how to start an Ethernet OAM remote-loopback mechanism:

Switch# ethernet oam remote-loopback start interface eth-0-1

**Related Commands**

show ethernet oam state-machine

---

**13.2.12 ethernet oam remote-loopback stop**

**Command Purpose**

Use this command to stop an Ethernet OAM remote-loopback process.

**Command Syntax**

```
ethernet oam remote-loopback stop interface IFNAME
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Name of the interface</td>
<td>Support physical ports</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

Use this command to stop an Ethernet OAM remote loopback mechanism.

**Usage**

Use this command to stop an Ethernet OAM remote loopback mechanism.

**Examples**

The following example shows how to stop an Ethernet OAM remote-loopback process:

Switch# ethernet oam remote-loopback stop interface eth-0-9

**Related Commands**

show ethernet oam state-machine
13.2.13  ethernet oam timeout

Command Purpose

Use this command to reset the LOCAL_LOST_LINK_TIMER and start an Ethernet OAM discovery process. Use the no form of the command to reset to the default value.

Command Syntax

ethernet oam timeout SECONDS
no ethernet oam timeout

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>The number of seconds chosen for the link-timer</td>
<td>2-30</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

The default value of the timeout is 5 seconds

Usage

This command is used to start a discovery process by resetting the LOCAL_LOST_LINK_TIMER.

Examples

The following example shows how to set the timeout to 5s:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ethernet oam timeout 5

Related Commands

None

13.2.14  ethernet oam remote-failure

Command Purpose

Use this command to error-disable port when get remote failure item form peer. Use the no form of the command to unset the action.

Command Syntax

ethernet oam remote-failure (link-fault | critical-event | dying-gasp) action error-disable-interface
no ethernet oam remote-failure (link-fault | critical-event | dying-gasp) action error-disable-interface

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>link-fault</td>
<td>Critical Link Event</td>
<td>-</td>
</tr>
<tr>
<td>critical-event</td>
<td>Dying Gasp Event</td>
<td>-</td>
</tr>
<tr>
<td>dying-gasp</td>
<td>Link Fault Event</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

None

Usage
This command is used to error-disable port when get remote failure item form peer.

**Examples**

The following example shows how to error-disable port when get remote failure item form peer on interface eth-0-1:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ethernet oam remote-failure link-fault action error-disable-interface

**Related Commands**
None

### 13.2.15 show ethernet oam discovery

**Command Purpose**

Use this command to display the ethernet oam administrative and operation configuration for local and remote DTE

**Command Syntax**

show ethernet oam discovery (interface IFNAME [])

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface IFNAME</td>
<td>Name of the interface</td>
<td>Support physical ports</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

The following sample output from this command displays ethernet oam administrative and operation configurations for local and remote DTE

**Examples**

The following example shows how to display the ethernet oam administrative and operation configuration for local and remote DTE of interface eth-0-1:

Switch1# show ethernet oam discovery interface eth-0-1

**Related Commands**
None

### 13.2.16 show Ethernet oam status

**Command Purpose**

Use this command to display the runtime settings of link-monitoring and general OAM operations for all interfaces or for a specific interface

**Command Syntax**

show ethernet oam status (interface IFNAME [])

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface IFNAME</td>
<td>Name of the interface</td>
<td>Support physical ports</td>
</tr>
</tbody>
</table>
**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

The following example shows how to display the runtime settings of link-monitoring and general OAM operations of interface eth-0-1:

```
Switch# show ethernet oam status interface eth-0-1
```

**Related Commands**

None

---

13.2.17 show ethernet oam state-machine

**Command Purpose**

Use this command to display the state machine information.

**Command Syntax**

```
show ethernet oam state-machine (interface IFNAME)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface IFNAME</td>
<td>Name of the interface</td>
<td>Support physical ports</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

The command displays the state of the interface.

**Examples**

The following example shows how to display the state machine information of eth-0-1:

```
Switch# show ethernet oam state-machine interface eth-0-1
```

**Related Commands**

None

---

13.2.18 show ethernet oam statistics

**Command Purpose**

Use this command to display the statistics information.

**Command Syntax**

```
show ethernet oam statistics (interface IFNAME)
```

www.fs.com
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface IFNAME</td>
<td>Name of the interface</td>
<td>Support physical ports</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

The command displays the statistics of the interface.

**Examples**

The following example shows how to display the statistics information of eth-0-1:

```
Switch# show ethernet oam statistics interface eth-0-1
```

**Related Commands**

None

### 13.3 CFM Commands

#### 13.3.1 ethernet cfm enable

**Command Purpose**

Use this command to enable CFM globally. Use the no parameter to disable the CFM function on the bridge.

**Command Syntax**

```
eternet cfm enable
no ethernet cfm enable
```

**Command Mode**

Global Configuration

**Default**

Disabled

**Usage**

This command is used to enable CFM globally.

**Examples**

The following example shows how to enable and disable cfm globally:

```
Switch# configure terminal
Switch(config)# ethernet cfm enable
Switch(config)# no ethernet cfm enable
```

**Related Commands**

None
13.3.2 ethernet cfm domain level

Command Purpose

Use this command to create an MD within which you can manage Ethernet traffic or enter cfm domain mode. Ensure you specify the level for each MD. The levels separate MDs from each other and provide different areas of functionality.

Command Syntax

```
ethernet cfm domain DOMAIN_NAME level LEVEL
no ethernet cfm domain DOMAIN_NAME
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAIN_NAME</td>
<td>Maintenance domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>LEVEL</td>
<td>MD level</td>
<td>0-7</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

The levels define the MD as follows:
- 0~2 (operator levels)
- 3~4 (provider levels)
- 5~7 (customer levels)

Examples

The following example shows how to create and destroy domain:

```
Switch# configure terminal
Switch(config)# ethernet cfm domain test 5
Switch(config-ether-cfm)# exit
Switch(config)# no ethernet cfm domain test
```

Related Commands

None

13.3.3 service

Command Purpose

Use this command to create an MA within which you can create mep.

Command Syntax

```
service CSI_ID (vlan VLAN_ID | )
no service CSI_ID
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSI_ID</td>
<td>Maintenance association name</td>
<td>MD(Maintenance domain) name and MA(Maintenance association) name totally up to 44 characters.</td>
</tr>
<tr>
<td>vlan VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
</tbody>
</table>
Command Mode
Ethernet-Cfm Configuration

Default
None

Usage
None

Examples
The following example shows how to create and remove MA:
Switch# configure terminal
Switch(config)# ethernet cfm domain test level 5
Switch(config-ether-cfm)# service cst vlan 30
Switch(config-ether-cfm)# no service cst

Related Commands
ethernet cfm domain DOMAIN_NAME level LEVEL

13.3.4 ethernet cfm mep
Command Purpose
Use this command to define an MEP within an MA. Each MEP and remote MEP must have a unique ID within an MA. If two or more MEPS share the same ID, CFM raises an event indicating a duplicate MEP exists in the MA.

Command Syntax
ethernet cfm mep ( down | up ) mpid MEPID domain DOMAIN_NAME ( vlan VLAN_ID | ) interval ( 1 | 2 | 3 | 4 | 5 | 6 | 7 )
no ethernet cfm mep ( down | up ) mpid MEPID domain DOMAIN_NAME ( vlan VLAN_ID | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>down</td>
<td>Down mep</td>
<td>-</td>
</tr>
<tr>
<td>up</td>
<td>Up mep</td>
<td>-</td>
</tr>
<tr>
<td>MEPID</td>
<td>Local mep id</td>
<td>1-8191</td>
</tr>
<tr>
<td>DOMAIN_NAME</td>
<td>Maintenance domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>vlan VLAN_ID</td>
<td>Vlan id, the range is 1 to 4094</td>
<td>1-4094</td>
</tr>
<tr>
<td>1</td>
<td>CCM Interval 3.3 millisecond</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>CCM Interval 10 millisecond</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>CCM Interval 100 millisecond</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>CCM Interval 1 second</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>CCM Interval 10 second</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>CCM Interval 1 minute</td>
<td>-</td>
</tr>
<tr>
<td>7</td>
<td>CCM Interval 10 minutes</td>
<td>-</td>
</tr>
</tbody>
</table>
Command Mode

Interface Configuration

Default

None

Usage

None

Examples

The following example shows how to create MEP:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ethernet cfm mep down mpid 1 domain md1 vlan 2 interval 1

Related Commands

ethernet cfm domain DOMAIN_NAME level LEVEL
service CSI_ID (vlan VLAN_ID)

13.3.5 ethernet cfm mep crosscheck mpid

Command Purpose

Use this command to define a remote MEP within an MA. Each MEP and remote MEP must have a unique ID within an MA. If two or more MEPs share the same ID, CFM raises an event indicating a duplicate MEP exists in the MA.

Command Syntax

ethernet cfm mep crosscheck mpid MEPID domain DOMAIN_NAME (vlan VLAN_ID |) ( mac MAC |)
no ethernet cfm mep crosscheck mpid MEPID domain DOMAIN_NAME (vlan VLAN_ID |)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEPID</td>
<td>The range is 1 to 8191</td>
<td>1-8191</td>
</tr>
<tr>
<td>DOMAIN_NAME</td>
<td>Maintenance domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>vlan VLAN_ID</td>
<td>Vlan id, the range is 1 to 4094</td>
<td>1-4094</td>
</tr>
<tr>
<td>MAC</td>
<td>Remote mep mac address</td>
<td>MAC Address</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

The following example shows how to create remote MEP:

Switch# configure terminal
Switch(config)# ethernet cfm domain test level 5
Switch(config-ether-cfm)# service cst vlan 30
Switch(config-ether-cfm)# exit
Switch(config)# interface eth-0-9
Switch(config-if)# ethernet cfm mep crosscheck mpid 8000 domain test vlan 30 mac 0.0.1

**Related Commands**

ethernet cfm domain DOMAIN_NAME level LEVEL
service CSI_ID (vlan VLAN_ID)

### 13.3.6  ethernet cfm mip

**Command Purpose**

Use this command to define an MIP. The relative MD and MA should be configured before MIP is configured.

**Command Syntax**

```
ethernet cfm mip level LEVEL vlan VLAN_ID
no ethernet cfm mip level LEVEL vlan VLAN_ID
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LEVEL</td>
<td>MD level, the range is 0 to 7</td>
<td>1-7</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

None

**Usage**

None

**Examples**

The following example shows how to create MIP:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ethernet cfm mip level 5 vlan 2
```

**Related Commands**

ethernet cfm domain DOMAIN_NAME level LEVEL
service CSI_ID (vlan VLAN_ID)

### 13.3.7  ethernet cfm cc enable domain

**Command Purpose**

Use the command to enable continuity check for an MA.

**Command Syntax**

```
ethernet cfm cc enable domain DOMAIN_NAME (vlan VLAN_ID |)
no ethernet cfm cc enable domain DOMAIN_NAME (vlan VLAN_ID |)
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAIN_NAME</td>
<td>Maintenance domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

None

**Usage**

None

**Examples**

The following example shows how to enable cc:

Switch# configure terminal
Switch(config)# ethernet cfm cc enable domain test vlan 2

**Related Commands**

- ethernet cfm domain DOMAIN_NAME level LEVEL
- service CSI_ID (vlan VLAN_ID)

13.3.8 ethernet cfm cc domain priority

**Command Purpose**

Use the command to define continuity check vlan priority for an MA.

**Command Syntax**

`ethernet cfm cc domain DOMAIN_NAME (vlan VLAN_ID ) priority VLAN_PRIORITY`

`no ethernet cfm cc domain DOMAIN_NAME (vlan VLAN_ID ) priority`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAIN_NAME</td>
<td>Maintenance domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
<tr>
<td>VLAN_PRIORITY</td>
<td>Vlan priority. The default value is 0</td>
<td>0-7</td>
</tr>
</tbody>
</table>
Examples

The following example shows how to configure vlan priority for CC message:

Switch# configure terminal
Switch(config)# ethernet cfm cc domain test vlan 2 priority 3

Related Commands

```
ethernet cfm domain DOMAIN_NAME level LEVEL
service CSI_ID (vlan VLAN_ID)
ethernet cfm cc enable domain DOMAIN_NAME (vlan VLAN_ID)
```

13.3.9 ethernet cfm loopback

Command Purpose

Use the command to issue CFM loopback messages for remote mepid or multicast address and verify that remote MEPs are accessible.

Command Syntax

```
ethernet cfm loopback (multicast | unicast) mepid MEPID (domain DOMAIN_NAME | level LEVEL) (vlan VLAN_ID) (repeat COUNT) (timeout TIMEOUT) (priority PRIORITY)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>Send multicast frame</td>
<td>-</td>
</tr>
<tr>
<td>unicast</td>
<td>Send unicast frame</td>
<td>-</td>
</tr>
<tr>
<td>RMEPID</td>
<td>Remote mep id</td>
<td>1-8191</td>
</tr>
<tr>
<td>MEPID</td>
<td>Source mep id</td>
<td>1-8191</td>
</tr>
<tr>
<td>domain</td>
<td>Maintenance domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>level</td>
<td>MD level</td>
<td>0-7</td>
</tr>
<tr>
<td>vlan</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
<tr>
<td>repeat</td>
<td>Repeat count, the default value is 1</td>
<td>1-255</td>
</tr>
<tr>
<td>timeout</td>
<td>The value of timeout, the default value is 5</td>
<td>1-65535 seconds</td>
</tr>
<tr>
<td>priority</td>
<td>The value of VLAN priority</td>
<td>0-7</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to start loopback:

Switch# ethernet cfm loopback multicast mepid 1 domain test vlan 2 repeat 3 timeout 5 priority 7
Related Commands

ethernet cfm mep (down|up) mepid MEPID domain DOMAIN_NAME (vlan VLAN_ID |) interval (1 | 2 | 3 | 4 | 5 | 6 | 7)
ethernet cfm mep crosscheck mepid MEPID (vlan VLAN_ID |) mac MAC

13.3.10  ethernet cfm loopback mac

Command Purpose

Use the command to issue CFM loopback messages for remote MEP or MIP mac address and verify that remote MEPs or MIPs are accessible.

Command Syntax

ethernet cfm loopback mac MACADDRESS unicast mepid MEPID ( domain DOMAIN_NAME | level LEVEL ) ( vlan VLAN_ID | ) ( repeat COUNT | ) ( timeout TIMEOUT | ) ( priority PRIORITY | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MACADDRESS</td>
<td>The remote mep mac address</td>
<td>MAC Address</td>
</tr>
<tr>
<td>MEPID</td>
<td>The source local mep id and its range is 1 to 8191</td>
<td>1-8191</td>
</tr>
<tr>
<td>domain DOMAIN_NAME</td>
<td>Maintenance domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>level LEVEL</td>
<td>MD level</td>
<td>0-7</td>
</tr>
<tr>
<td>vlan VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
<tr>
<td>repeat COUNT</td>
<td>Repeat count, the range is 1 to 255, the default value is 1</td>
<td>1-255</td>
</tr>
<tr>
<td>timeout TIMEOUT</td>
<td>The value of timeout, the default value is 5</td>
<td>1-65535 seconds</td>
</tr>
<tr>
<td>priority PRIORITY</td>
<td>The value of VLAN priority</td>
<td>0-7</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to start loopback:

Switch# ethernet cfm loopback mac 0.0.1 unicast mepid 1 domain test vlan 2 repeat 3 timeout 5 priority 7

Related Commands

ethernet cfm mep (down|up) mepid MEPID domain DOMAIN_NAME (vlan VLAN_ID |) interval (1 | 2 | 3 | 4 | 5 | 6 | 7)
ethernet cfm mep crosscheck mepid MEPID (vlan VLAN_ID |) mac MAC
13.3.11  *ethernet cfm errors enable domain*

**Command Purpose**

Use the command to configure reserve ccm errors. The default action is to reserve ccm errors.

**Command Syntax**

```
ethernet cfm errors enable domain DOMAIN_NAME (vlan VLAN_ID |)
no ethernet cfm errors enable domain DOMAIN_NAME (vlan VLAN_ID |)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAIN_NAME</td>
<td>Maintenance domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>vlan VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

None

**Usage**

For every mep, five latest errors will be reserved.

**Examples**

The following example shows how to configure reserve ccm errors:

```
Switch# configure terminal
Switch(config)# ethernet cfm errors enable domain test vlan 2
```

**Related Commands**

None

13.3.12  *clear ethernet cfm errors*

**Command Purpose**

Use the command to clear cfm errors for domain.

**Command Syntax**

```
clear ethernet cfm errors (domain DOMAIN_NAME | level LEVEL )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain DOMAIN_NAME</td>
<td>Maintenance domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>level LEVEL</td>
<td>MD level</td>
<td>0-7</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None
Examples

The following example shows how to clear ccm errors:
Switch# clear ethernet cfm errors domain test

Related Commands

None

13.3.13 ethernet cfm ais status enable

Command Purpose

Use the command to enable or disable ais function and configure relative parameters.

Command Syntax

ethernet cfm ais status enable ( all | loc | mismerge | unexpected-mep | unexpected-meg-level | unexpected-period ) domain
DOMAIN_NAME ( vlan VLAN_ID )
level LEVEL ( unicast RMEP_MAC | multicast ) ( cvlan VLAN_LIST )
no ethernet cfm ais status enable ( all | loc | mismerge | unexpected-mep | unexpected-meg-level | unexpected-period ) domain
DOMAIN_NAME ( vlan VLAN_ID )
level LEVEL ( unicast RMEP_MAC | multicast )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Ais for all defect condition</td>
<td>-</td>
</tr>
<tr>
<td>loc</td>
<td>Ais for loss of continuity</td>
<td>-</td>
</tr>
<tr>
<td>mismerge</td>
<td>Ais for incorrect MEG ID</td>
<td>-</td>
</tr>
<tr>
<td>unexpected-mep</td>
<td>Ais for unexpected MEP ID received</td>
<td>-</td>
</tr>
<tr>
<td>unexpected-meg-level</td>
<td>Ais for incorrect MEG level</td>
<td>-</td>
</tr>
<tr>
<td>unexpected-period</td>
<td>Ais for mis-matched in period received</td>
<td>-</td>
</tr>
<tr>
<td>DOMAIN_NAME</td>
<td>Maintenance domain name of the local mep</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>vlan VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
<tr>
<td>LEVEL</td>
<td>Ais packet will be sent in this MD level</td>
<td>1-7</td>
</tr>
<tr>
<td>unicast</td>
<td>Unicast ais frame to be sent</td>
<td>-</td>
</tr>
<tr>
<td>RMEP_MAC</td>
<td>The remote mep mac address</td>
<td>-</td>
</tr>
<tr>
<td>multicast</td>
<td>Multicast ais frame to be sent</td>
<td>-</td>
</tr>
<tr>
<td>cvlan VLAN_LIST</td>
<td>Cvlan id of ais packet</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

None
Usage
None

Examples
The following example shows how to configure ais:
```
Switch# configure terminal
Switch(config)# ethernet cfm ais status enable all domain test vlan 2 level 5 multicast
```

Related Commands
None

13.3.14 ethernet cfm ais suppress alarm enable domain

Command Purpose
Use the command to enable ais suppress alarm. When this command is configured and ais condition is enabled, the loc errors will not be reported.

Command Syntax
```
ethernet cfm ais suppress alarm enable domain DOMAIN_NAME (vlan VLAN_ID | )
no ethernet cfm ais suppress alarm enable domain DOMAIN_NAME (vlan VLAN_ID | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAIN_NAME</td>
<td>Maintenance domain name of the local mep</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>vlan VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
None

Examples
The following example shows how to enable ais suppress alarm:
```
Switch# configure terminal
Switch(config)# ethernet cfm ais suppress alarm enable domain test vlan 2
```

Related Commands
None

13.3.15 ethernet cfm server-ais status enable level

Command Purpose
Use this command to configure ais server and parameters.
Command Syntax

ethernet cfm server-ais status enable level LEVEL ( interval ( 1 | 60 ) )
no ethernet cfm server-ais status enable

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LEVEL</td>
<td>Ais packet will be sent in this MD level</td>
<td>1-7</td>
</tr>
<tr>
<td>interval (1</td>
<td>60)</td>
<td>Transmission interval for AIS frames, the default value is 1 second</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

The following example shows how to configure ais server:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ethernet cfm server-ais status enable level 5 interval 60

Related Commands

None

13.3.16 show ethernet cfm domain

Command Purpose

Use the command to display information related to the configuration of MDs and MAs.

Command Syntax

show ethernet cfm domain DOMAIN_NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAIN_NAME</td>
<td>Maintenance domain name</td>
<td>String with up to 43 characters</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None
The following example shows how to display information related to the configuration of MDs and Mas:

Switch# show ethernet cfm domain test

Related Commands
None

### 13.3.17 show ethernet cfm maintenance-points

**Command Purpose**
Use the command to display information related to configuration of MEPs, remote MEPs, and MIPs.

**Command Syntax**
show ethernet cfm maintenance-points

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
The following example shows how to display information related to configuration of MEPs, remote MEPs, and MIPs:

Switch# show ethernet cfm maintenance-points

Related Commands
None

### 13.3.18 show ethernet cfm maintenance-points local

**Command Purpose**
Use the command to display information related to configuration of MEPs and MIPs.

**Command Syntax**
show ethernet cfm maintenance-points local (mep | mip) (interface IFNAME | domain DOMAIN_NAME | level LEVEL)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mep</td>
<td>Maintenance end point</td>
<td>-</td>
</tr>
<tr>
<td>mip</td>
<td>Maintenance intermediate point</td>
<td>-</td>
</tr>
<tr>
<td>interface IFNAME</td>
<td>Interface name</td>
<td>Support physical ports</td>
</tr>
<tr>
<td>domain DOMAIN_NAME</td>
<td>Maintenance domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>level LEVEL</td>
<td>MD level</td>
<td>0-7</td>
</tr>
</tbody>
</table>
Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following example shows how to display information related to configuration of MEPs and MIPs:
Switch# show ethernet cfm maintenance-points local mep interface eth-0-1

Related Commands
None

13.3.19 show ethernet cfm maintenance-points remote

Command Purpose
Use the command to display information related to configuration of remote MEPs.

Command Syntax
show ethernet cfm maintenance-points remote ( mpid MEPID | mac MAC | ) ( domain DOMAIN_NAME | level LEVEL | ) ( vlan VLAN_ID | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpid MEPID</td>
<td>The remote mep id</td>
<td>1-8191</td>
</tr>
<tr>
<td>mac MAC</td>
<td>The remote mep mac address</td>
<td>MAC Address</td>
</tr>
<tr>
<td>domain DOMAIN_NAME</td>
<td>Maintenance domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>level LEVEL</td>
<td>MD level, the range is 0 to 7</td>
<td>0-7</td>
</tr>
<tr>
<td>vlan VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following example shows how to display information of remote MEP:
Switch# show ethernet cfm maintenance-points remote mpid 1 domain test

Related Commands
None
13.3.20  show ethernet cfm cc config

Command Purpose
Use the command to display information related to CC configuration.

Command Syntax
show ethernet cfm cc config

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following example shows how to display information related to CC configuration:
Switch# show ethernet cfm cc config

Related Commands
None

13.3.21  show ethernet cfm errors

Command Purpose
Use the command to display CFM error.

Command Syntax
show ethernet cfm errors ( domain DOMAIN_NAME | level LEVEL )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain</td>
<td>Maintenance domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>level LEVEL</td>
<td>MD level, the range is 0 to 7</td>
<td>0-7</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following example shows how to display CFM error:
Switch# show ethernet cfm errors

Related Commands
None
13.3.22  show ethernet cfm ais mep

Command Purpose
Use the command to display ais configuration for local mep.

Command Syntax
show ethernet cfm ais mep MEPID domain DOMAIN_NAME ( vlan VLAN_ID | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEPID</td>
<td>Local mep id, the range is 1 to 8191</td>
<td>1-8191</td>
</tr>
<tr>
<td>DOMAIN_NAME</td>
<td>Maintenance domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>vlan VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following example shows how to display ais configuration for local mep:
Switch# show ethernet cfm ais mep 1 domain test vlan 2

Related Commands
None

13.3.23  show ethernet cfm

Command Purpose
Use the command to display cfm global information.

Command Syntax
show ethernet cfm

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following example shows how to cfm global information:
Switch# show ethernet cfm

Related Commands
None
13.3.24  ethernet cfm linktrace rmepid

Command Purpose

Use the command to issue CFM linktrace messages for remote mep and discovery a path to remote mep.

Command Syntax

ethernet cfm linktrace rmepid RMEPID ( domain DOMAIN_NAME | level LEVEL ) ( vlan VLAN_ID | ) ( ttl TTL | timeout TIMEOUT | priority PRIORITY | ltm-egress-identifier-tlv | sender-id-tlv | organization-specific-tlv )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RMEPID</td>
<td>Remote mep id</td>
<td>1-8191</td>
</tr>
<tr>
<td>MEPID</td>
<td>The source local mep id</td>
<td>1-8191</td>
</tr>
<tr>
<td>domain DOMAIN_NAME</td>
<td>Maintenance domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>level LEVEL</td>
<td>MD level, the range is 0 to 7</td>
<td>0-7</td>
</tr>
<tr>
<td>vlan VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
<tr>
<td>ttl TTL</td>
<td>Maximum hops, the default value is 64</td>
<td>1-255</td>
</tr>
<tr>
<td>timeout TIMEOUT</td>
<td>The value of timeout, the default value is 5</td>
<td>1-65535</td>
</tr>
<tr>
<td>priority PRIORITY</td>
<td>Vlan priority, the default value is 7</td>
<td>0-7</td>
</tr>
<tr>
<td>ltm-egress-identifier-tlv</td>
<td>LTM egress identifier TLV</td>
<td>-</td>
</tr>
<tr>
<td>sender-id-tlv</td>
<td>Sender ID TLV</td>
<td>-</td>
</tr>
<tr>
<td>organization-specific-tlv</td>
<td>Organization Specific TLV</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to start linktrace:
Switch# ethernet cfm linktrace rmepid 1 mepid 2 domain test vlan 2 ttl 255 timeout 5 priority 7

Related Commands

ethernet cfm mep (down|up) mpid MEPID domain DOMAIN_NAME (vlan VLAN_ID |) interval (1 | 2 | 3 | 4 | 5 | 6 | 7)
ethernet cfm mep crosscheck mpid MEPID (vlan VLAN_ID |) (mac MAC)
### 13.3.25 ethernet cfm linktrace mac

**Command Purpose**

Use the command to issue CFM linktrace messages for remote mep or mip mac address and discovery a path to remote mep or mip.

**Command Syntax**

```
ethernet cfm linktrace mac MACADDRESS mepid MEPID ( domain DOMAIN_NAME | level LEVEL ) ( vlan VLAN_ID | ) ( ttl TTL | timeout TIMEOUT | priority PRIORITY )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MACADDRESS</td>
<td>The remote mep mac address</td>
<td>MAC Address</td>
</tr>
<tr>
<td>MEPID</td>
<td>The source local mep id</td>
<td>1-8191</td>
</tr>
<tr>
<td>domain DOMAIN_NAME</td>
<td>Maintenance domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>level LEVEL</td>
<td>MD level, the range is 0 to 7</td>
<td>0-7</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
<tr>
<td>ttl TTL</td>
<td>Maximum hops, the default value is 64</td>
<td>1-255</td>
</tr>
<tr>
<td>timeout TIMEOUT</td>
<td>The value of timeout, the default value is 5</td>
<td>1-65535</td>
</tr>
<tr>
<td>priority PRIORITY</td>
<td>Vlan priority, the default value is 7</td>
<td>0-7</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

The following example shows how to start linktrace:

```
Switch# ethernet cfm linktrace mac 7234.ef5a.2806 mepid 1 domain test vlan 2 ttl 255 timeout 5 priority 7
```

**Related Commands**

- `ethernet cfm mep (down|up) mpid MEPID domain DOMAIN_NAME (vlan VLAN_ID |)` interval (1 | 2 | 3 | 4 | 5 | 6 | 7)
- `ethernet cfm mep crosscheck mpid MEPID (vlan VLAN_ID |)` (mac MAC)

### 13.3.26 ethernet cfm linktrace cache enable

**Command Purpose**

Use the command to configure caching linktrace information. The default value is disabled.

**Command Syntax**

```
ethernet cfm linktrace cache enable
no ethernet cfm linktrace cache enable
```
**Command Mode**
Global Configuration

**Default**
Disabled

**Usage**
None

**Examples**
The following example shows how to configure caching linktrace information:
```
Switch# configure terminal
Switch(config)# ethernet cfm linktrace cache enable
```

**Related Commands**
None

**13.3.27 ethernet cfm linktrace cache size**

**Command Purpose**
Use the command to configure linktrace cache size.

**Command Syntax**
```
ethernet cfm linktrace cache size
no ethernet cfm linktrace cache size
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENTRIES</td>
<td>Cache entry number, the default value is 100</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
100

**Usage**
None

**Examples**
The following example shows how to configure linktrace cache size:
```
Switch# configure terminal
Switch(config)# ethernet cfm linktrace cache size 200
```

**Related Commands**
None
### 13.3.28 ethernet cfm linktrace cache holdtime

**Command Purpose**
Use the command to configure linktrace cache hold time.

**Command Syntax**
ethernet cfm linktrace cache holdtime MINUTES

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MINUTES</td>
<td>Cache entry hold time minutes, the default value is 60 minutes</td>
<td>1-65535 minutes</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
60 minutes

**Usage**
None

**Examples**
The following example shows how to configure linktrace cache hold time:

```bash
Switch# configure terminal
Switch(config)# ethernet cfm linktrace cache holdtime 90
```

**Related Commands**
None

### 13.3.29 show ethernet cfm linktrace cache

**Command Purpose**
Use the command to display linktrace cache entries.

**Command Syntax**
show ethernet cfm linktrace cache

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
The following example shows how to display linktrace cache entries:

```bash
Switch# configure terminal
Switch(config)# ethernet cfm linktrace cache holdtime 90
```

**Related Commands**
None
13.3.30 clear ethernet cfm linktrace cache

Command Purpose
Use the command to clear linktrace cache.

Command Syntax
clear ethernet cfm linktrace cache

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following example shows how to clear linktrace cache:
Switch# show ethernet cfm linktrace cache

Related Commands
None

13.3.31 ethernet cfm mip ccm-database size

Command Purpose
Use the command to configure mip ccm database size.

Command Syntax
ethernet cfm mip ccm-database size ENTRIES
no ethernet cfm mip ccm-database size

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENTRIES</td>
<td>Cache entry number, the range is 1 to 65535, the default value is 100</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
100

Usage
None

Examples
The following example shows how to configure mip ccm database size:
Switch# configure terminal
Switch(config)# ethernet cfm mip ccm-database size 200

Related Commands
None
13.3.32  ethernet cfm mip ccm-database holdtime

**Command Purpose**

Use the command to configure mip ccm-database hold time.

**Command Syntax**

```
ethernet cfm mip ccm-database holdtime MINUTES
no ethernet cfm mip ccm-database holdtime
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MINUTES</td>
<td>Mip ccm database hold time</td>
<td>1-65535 minutes</td>
</tr>
<tr>
<td></td>
<td>minutes, the range is 60 to 65535</td>
<td></td>
</tr>
<tr>
<td></td>
<td>minutes, the default value is 60</td>
<td></td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

60 minutes

**Usage**

None

**Examples**

The following example shows how to configure mip ccm-database hold time:

```
Switch# configure terminal
Switch(config)# ethernet cfm mip ccm-database holdtime 90
```

**Related Commands**

None

---

13.3.33  show ethernet cfm mip ccm-database

**Command Purpose**

Use the command to display mip ccm-database.

**Command Syntax**

```
show ethernet cfm mip ccm-database
```

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

The following example shows how to display mip ccm-database:

```
Switch# show ethernet cfm mip ccm-database
```

**Related Commands**

None
13.3.34 clear ethernet cfm mip ccm-database

**Command Purpose**
Use the command to clear mip ccm database.

**Command Syntax**
clear ethernet cfm mip ccm-database

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
The following example shows how to clear mip ccm database:
```
Switch# clear ethernet cfm mip ccm-database
```

**Related Commands**
None

13.3.35 ethernet cfm sf-reason

**Command Purpose**
Use the command to configure signal fail reasons and these reasons will trigger g8031/g8032.

**Command Syntax**
```
ethernet cfm sf-reason ( all | { loc | rdi-rx | ais-defect } | none )
```
```
no Ethernet cfm sf-reason
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Configure all reasons to trigger Signal Fail</td>
<td>-</td>
</tr>
<tr>
<td>loc</td>
<td>Configure loc to trigger Signal Fail</td>
<td>-</td>
</tr>
<tr>
<td>rdi-rx</td>
<td>Configure remote mep rdi to trigger Signal Fail</td>
<td>-</td>
</tr>
<tr>
<td>ais-defect</td>
<td>Configure ais condition to trigger Signal Fail</td>
<td>-</td>
</tr>
<tr>
<td>none</td>
<td>Configure none reason</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
The default value of sf-reason is Loc
**Usage**
None

**Examples**
The following example shows how to configure signal fail reasons:
Switch# configure terminal
Switch(config)# ethernet cfm sf-reason all

**Related Commands**
None

13.3.36  ethernet cfm mode

**Command Purpose**
Use this command to configure cfm mode globally. Use the no parameter to configure cfm mode to 802.1ag.

**Command Syntax**

```
ethernet cfm mode ( dot1ag | y1731 )
no ethernet cfm mode
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1ag</td>
<td>IEEE 802.1ag-2007</td>
<td>-</td>
</tr>
<tr>
<td>y1731</td>
<td>ITU-T.Y.1731</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
IEEE 802.1ag-2007

**Usage**
None

**Examples**
The following example shows how to configure cfm mode globally:
Switch# configure terminal
Switch(config)# ethernet cfm mode dot1ag
Switch(config)# no ethernet cfm mode

**Related Commands**
None

13.3.37  ethernet cfm lm enable dual-ended

**Command Purpose**
Use this command to enable dual-ended loss measurement.

**Command Syntax**

```
ethernet cfm lm enable dual-ended ( domain DOMAIN_NAME | level LEVEL ) ( vlan VLAN_ID | ) mepid MEPID ( all-cos | per-cos | cos COS_VALUE ) ( stats-interval INTERVAL_VALUE ) ( cache-size CACHE VALUE )
no ethernet cfm lm enable dual-ended ( domain DOMAIN_NAME | level LEVEL ) ( vlan VLAN_ID | ) mepid MEPID
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAIN_NAME</td>
<td>Maintenance domain name</td>
<td>String</td>
</tr>
<tr>
<td>LEVEL</td>
<td>MD level</td>
<td>0-7</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
<tr>
<td>MEPID</td>
<td>Local mep id</td>
<td>1-8191</td>
</tr>
<tr>
<td>all-cos</td>
<td>All packets with different cos will be counted together</td>
<td>-</td>
</tr>
<tr>
<td>per-cos</td>
<td>Packets with different cos will be counted separately</td>
<td>-</td>
</tr>
<tr>
<td>cos COS_VALUE</td>
<td>Packets with specified cos will be counted.</td>
<td>0-7</td>
</tr>
<tr>
<td>stats-interval</td>
<td>After an interval, system will get counter values and calculate frame loss and frame loss ratio for near end and far end. After an interval, system will get counter values and calculate frame loss and frame loss ratio for near end and far end. The range is 1 to 10, unit is second, and the default value is 1.</td>
<td>1-10 seconds</td>
</tr>
<tr>
<td>cache-size</td>
<td>Cache entry number for lm results.</td>
<td>1-512</td>
</tr>
<tr>
<td>CACHE VALUE</td>
<td>Cache entry number for lm results.</td>
<td>The default value is 128.</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

None

**Usage**

None

**Examples**

The following example shows how to enable dual-ended loss measurement:

```
Switch# configure terminal
Switch(config)# ethernet cfm lm enable dual-ended domain md1 vlan 2 mepid 1 all-cos stats-interval 1 cache-count 256
```

**Related Commands**

None
13.3.38 ethernet cfm lm enable single-ended

**Command Purpose**
Use this command to enable single-ended loss measurement.

**Command Syntax**
```
ethernet cfm lm enable single-ended ( domain DOMAIN_NAME | level LEVEL ) ( vlan VLAN_ID | ) mepid MEPID ( all-cos | per-cos | cos COS_VALUE )
```
```
no ethernet cfm lm enable single-ended ( domain DOMAIN_NAME | level LEVEL ) ( vlan VLAN_ID | ) mepid MEPID
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAIN_NAME</td>
<td>Maintenance domain name</td>
<td>String up to 43 characters</td>
</tr>
<tr>
<td>LEVEL</td>
<td>MD leve</td>
<td>0-7</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
<tr>
<td>MEPID</td>
<td>Local mep id</td>
<td>1-8191</td>
</tr>
<tr>
<td>all-cos</td>
<td>All packets with different cos will be counted together</td>
<td>-</td>
</tr>
<tr>
<td>per-cos</td>
<td>Packets with different cos will be counted separately</td>
<td>-</td>
</tr>
<tr>
<td>cos COS_VALUE</td>
<td>Packets with specified cos will be counted.</td>
<td>0-7</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
None

**Usage**
None

**Examples**
The following example shows how to enable single-ended loss measurement:
```
Switch# configure terminal
Switch(config)# ethernet cfm lm enable single-ended domain md1 vlan 2 mepid 1 all-cos
```

**Related Commands**
None

13.3.39 ethernet cfm lm single-ended

**Command Purpose**
Use the command to issue CFM single-ended loss message messages.

**Command Syntax**
```
ethernet cfm lm single-ended ( domain DOMAIN_NAME | level LEVEL ) ( vlan VLAN_ID | ) rmepid RMEPID mepid MEPID ( count COUNT | ) ( interval ( 1 | 2 | 3 ) )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAIN_NAME</td>
<td>Maintenance domain name</td>
<td>-</td>
</tr>
<tr>
<td>LEVEL</td>
<td>MD leve</td>
<td>0-7</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
<tr>
<td>RMEPID</td>
<td>Remote mep id</td>
<td>1-8191</td>
</tr>
<tr>
<td>MEPID</td>
<td>Local mep id</td>
<td>1-8191</td>
</tr>
<tr>
<td>count COUNT</td>
<td>Repeat count, the default value is 2</td>
<td>2-60</td>
</tr>
<tr>
<td>interval</td>
<td>LM Transmission interval, default value is 1 second.</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>LM Interval, 100 milliseconds</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>LM Interval, 1 second</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>LM Interval, 10 seconds</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
The following example shows how to issue CFM single-ended loss message messages:

```
Switch# ethernet cfm lm single-ended domain md1 vlan 2 rme pid 2 mep id 1 count 10 interval 1
```

**Related Commands**
None

13.3.40 show ethernet cfm lm

**Command Purpose**
Use the command to display dual-ended loss measurement results.

**Command Syntax**

```
show ethernet cfm lm domain DOMAIN_NAME ( vlan VLAN_ID | ) mep id MEPID ( cos COS_VALUE )
```
### Command Mode

Privileged EXEC

### Default

None

### Usage

None

### Examples

The following example shows how to display dual-ended l2m results:

Switch# show ethernet cfm l2m domain md1 vlan 2 mepid 3

<table>
<thead>
<tr>
<th>DOMAIN</th>
<th>VLAN</th>
<th>MEPID</th>
<th>Start Time</th>
<th>End Time</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>md1</td>
<td>2</td>
<td>1</td>
<td>2013/07/15 9:00:09</td>
<td>2013/07/15 9:00:09</td>
<td>1. When the difference of Tx is less than the difference of Rx, the node is invalid, loss and loss ratio should be &quot;.-&quot;; 2. When loc is reported for mep, the loss should be &quot;.-&quot; and loss ratio should be 100%; 3. When calculate average loss and loss ratio, invalid or loc nodes will be excluded;</td>
</tr>
</tbody>
</table>

Latest dual-ended loss statistics:

<table>
<thead>
<tr>
<th>Index</th>
<th>Cos</th>
<th>Local-loss</th>
<th>Local-loss ratio</th>
<th>Remote-loss</th>
<th>Remote-loss ratio</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>all</td>
<td>4</td>
<td>050.0000%</td>
<td>4</td>
<td>050.0000%</td>
<td>09:00:09</td>
</tr>
<tr>
<td>2</td>
<td>all</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>- 09:00:09</td>
</tr>
<tr>
<td>3</td>
<td>all</td>
<td>0</td>
<td>000.0000%</td>
<td>100</td>
<td>100.0000%</td>
<td>09:00:09</td>
</tr>
<tr>
<td>4</td>
<td>all</td>
<td>0</td>
<td>000.0000%</td>
<td>99</td>
<td>099.0000%</td>
<td>09:00:09</td>
</tr>
<tr>
<td>5</td>
<td>all</td>
<td>0</td>
<td>000.0000%</td>
<td>90</td>
<td>090.0000%</td>
<td>09:00:09</td>
</tr>
<tr>
<td>6</td>
<td>all</td>
<td>0</td>
<td>000.0000%</td>
<td>1</td>
<td>001.0000%</td>
<td>09:00:09</td>
</tr>
<tr>
<td>7</td>
<td>all</td>
<td>0</td>
<td>000.0000%</td>
<td>0</td>
<td>000.0000%</td>
<td>09:00:09</td>
</tr>
<tr>
<td>8</td>
<td>all</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>- 09:00:09</td>
</tr>
</tbody>
</table>
13.3.41 ethernet cfm sd-reason

Command Purpose
Use the command to configure signal defect reasons. If dual-lm loss ration is greater than limit, log will be printed and trap will be reported.

Command Syntax
```
ethernet cfm sd-reason ( domain DOMAIN_NAME | level LEVEL ) ( vlan VLAN_ID | ) mepid MEPID ratio RATIO_VALUE
no ethernet cfm sd-reason ( domain DOMAIN_NAME | level LEVEL ) ( vlan VLAN_ID | ) mepid MEPID
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAIN_NAME</td>
<td>Maintenance domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>LEVEL</td>
<td>MD level</td>
<td>0-7</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
<tr>
<td>MEPID</td>
<td>Local mep id</td>
<td>1-8191</td>
</tr>
<tr>
<td>RATIO_VALUE</td>
<td>Dual-lm loss ratio limitation, the range is 1 to 1000, unit is one in a thousand,</td>
<td>1-1000</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
None
Examples

The following example shows how to enable sd-reason:

```
Switch# configure terminal
Switch(config)# ethernet cfm sd-reason domain md1 vlan 2 mepid 1 ratio 100
```

Related Commands

None

13.3.42 ethernet cfm (1dm|dmm)

Command Purpose

Use the command to issue CFM 1dm or dmm messages for remote mepid, receive dmr from remote mep, calculate and display frame delay.

Command Syntax

```
ethernet cfm (1dm | dmm) rmepid RMEPID mepid MEPID count COUNT ( domain DOMAIN_NAME | level LEVEL ) ( vlan VLAN_ID ) ( priority PRIORITY | interval (1 | 2 | 3 ) ) ( frame_size SIZE )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RMEPID</td>
<td>Remote mep id</td>
<td>1-8191</td>
</tr>
<tr>
<td>MEPID</td>
<td>Local mep id</td>
<td>1-8191</td>
</tr>
<tr>
<td>COUNT</td>
<td>Repeat count</td>
<td>1-60</td>
</tr>
<tr>
<td>DOMAIN_NAME</td>
<td>Maintenance domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
<tr>
<td>LEVEL</td>
<td>MD level</td>
<td>0-7</td>
</tr>
<tr>
<td>priority PRIORITY</td>
<td>Vlan priority, the default value is 7</td>
<td>0-7</td>
</tr>
<tr>
<td>interval</td>
<td>DM Transmission interval, default value is 1 second.</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>DM Interval, 100 milliseconds</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>DM Interval, 1 second</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>DM Interval, 10 seconds</td>
<td>-</td>
</tr>
<tr>
<td>frame_size SIZE</td>
<td>The range of SIZE should be 64 bytes to 9600 bytes, the default value is 64 bytes</td>
<td>64-9600 bytes</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None
Usage

None

Examples

The following example shows how to issue CFM 1dm or dmm messages:
Switch# configure terminal
Switch(config)# ethernet cfm dmm mepid 1 rmepid 2 duration 5 domain md1 vlan 2 priority 3 interval 1

Related Commands

None

13.3.43 ethernet cfm delaymeasurement cache enable

Command Purpose

Use the command to configure caching delaymeasurement information. The default value is enabled.

Command Syntax

ethernet cfm delaymeasurement cache enable
no ethernet cfm delaymeasurement cache enable

Command Mode

Global Configuration

Default

Enabled

Usage

None

Examples

The following example shows how to configure delaymeasurement cache enable:
Switch# configure terminal
Switch(config)# ethernet cfm delaymeasurement cache enable

Related Commands

None

13.3.44 ethernet cfm delaymeasurement cache size

Command Purpose

Use the command to configure delaymeasurement cache size.

Command Syntax

ethernet cfm delaymeasurement cache size ENTRIES
no Ethernet cfm delaymeasurement cache size

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENTRIES</td>
<td>Cache entry number, the default value is 1000</td>
<td>1-65535</td>
</tr>
</tbody>
</table>
Command Mode
Global Configuration

Default
1000

Usage
None

Examples
The following example shows how to configure delay measurement cache size:
Switch# configure terminal
Switch(config)# ethernet cfm delaymeasurement cache size 100

Related Commands
None

13.3.45 show ethernet cfm delaymeasurement cache

Command Purpose
Use the command to display delay measurement cache entries.

Command Syntax
show ethernet cfm delaymeasurement cache

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following example shows how to display delay measurement cache entries:
Switch# show ethernet cfm delaymeasurement cache

Related Commands
None

13.3.46 clear ethernet cfm delaymeasurement cache

Command Purpose
Use the command to clear delay measurement cache entries.

Command Syntax
clear ethernet cfm delaymeasurement cache

Command Mode
Privileged EXEC
Default
None

Usage
None

Examples
The following example shows how to clear delay measurement cache entries:
Switch# clear ethernet cfm delaymeasurement cache

Related Commands
None

13.3.47 ethernet cfm csf

Command Purpose
Use this command to configure CSF (client signal fail) relation between client MEP and server MEP.

Command Syntax
ethernet cfm csf client domain CLI_DOMAIN_NAME (vlan CLI_VLAN_ID |) mepid CLI_MEPID server domain SRV_DOMAIN_NAME (vlan SRV_VLAN_ID |) mepid SRV_MEPID (tx-interval (1 | 60) |)
no ethernet cfm csf client domain CLI_DOMAIN_NAME (vlan CLI_VLAN_ID |) mepid CLI_MEPID server domain SRV_DOMAIN_NAME (vlan SRV_VLAN_ID |) mepid SRV_MEPID

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI_DOMAIN_NAME</td>
<td>Client maintenance domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>vlan CLI_VLAN_ID</td>
<td>Client vlan id</td>
<td>1-4094</td>
</tr>
<tr>
<td>CLI_MEPID</td>
<td>Client local mep id</td>
<td>1-8191</td>
</tr>
<tr>
<td>SRV_DOMAIN_NAME</td>
<td>Server maintenance domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>vlan SRV_VLAN_ID</td>
<td>Server vlan id</td>
<td>1-4094</td>
</tr>
<tr>
<td>SRV_MEPID</td>
<td>Server local mep id</td>
<td>1-8191</td>
</tr>
<tr>
<td>tx-interval</td>
<td>Transmission interval of cfm</td>
<td>1 or 60 seconds</td>
</tr>
<tr>
<td></td>
<td>message, the default value</td>
<td></td>
</tr>
<tr>
<td></td>
<td>is 60 seconds</td>
<td></td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
None

Examples
The following example shows how to configure CSF relation:
Switch# configure terminal
Switch(config)# ethernet cfm csf client domain cust vlan 30 mepid 88 server domain provid vlan 20 mepid 666 tx-interval 1

Related Commands
None
13.3.48  show ethernet cfm csf

Command Purpose
Use the command to display csf relation and status.

Command Syntax
show ethernet cfm csf

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following example shows how to display csf:

Switch# show ethernet cfm csf
En-CSF Enable, Y(Yes)/N(No)
CTR-Client Trigger reason, L(los)/F(fdi)/R(rdi)/N(null)
ECC-Enter CSF Condition, Y(Yes)/N(No)
SRR-Server Rx Reason, L(los)/F(fdi)/R(rdi)/D(dci)/N(null)
Tx-I, Transmit Interval
Rx-I, The period which is gotten from LCK packets
Client Mep Server Mep
MPID Cli-Domain VLAN CTR ECC MPID Srv-Domain VLAN SRR Tx-I Rx-I
1003 md1234567890 3001 L/F/R Y 1004 md1234567890 2001 L/F/R 1 1

Related Commands
None

13.3.49  ethernet cfm lck enable

Command Purpose
Use this command to lock data packets for mep.

Command Syntax
ethernet cfm lck enable mep MEPID domain DOMAIN_NAME (vlan VLAN_ID |) tx-level TX_LEVEL ( { tx-interval (1 | 60) | cvlan VLAN_LIST } |)
no ethernet cfm lck enable mep MEPID domain DOMAIN_NAME (vlan VLAN_ID |)

Command Mode
Interface Configuration
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAIN_NAME</td>
<td>Maintenance domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>vlan VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
<tr>
<td>MEPID</td>
<td>Local mep id</td>
<td>1-8191</td>
</tr>
<tr>
<td>TX_LEVEL</td>
<td>Transmission level of lck message</td>
<td>0-7</td>
</tr>
<tr>
<td>tx-interval (1</td>
<td>60)</td>
<td>Transmission interval of lck message, the default value is 60 seconds</td>
</tr>
<tr>
<td>cvlan VLAN_LIST</td>
<td>Cvlan id of lck packet</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

**Default**
None

**Usage**
None

**Examples**
The following example shows how to enable lock data packets for mep:
```
Switch# configure terminal
Switch(config)# ethernet cfm lck enable domain md1 vlan 2 mepid 1 tx-level 5 tx-interval 1
```

**Related Commands**
None

---

**13.3.50  show ethernet cfm lck**

**Command Purpose**
Use the command to display lck information.

**Command Syntax**
```
show ethernet cfm lck
```

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
The following example shows how to display lck information:
```
Switch# show ethernet cfm lck
En-LCK Enable, Y(Yes)/N(No)
Rx-LC, Receive LCK packets and enter LCK condition, Y(Yes)/N(No)
```
Rx-I, The period which is gotten from LCK packets
Tx-Domain, frames with ETH-LCK information are sent to this Domain
Tx-I, Transmit Interval

<table>
<thead>
<tr>
<th>MPID</th>
<th>Domain</th>
<th>VLAN</th>
<th>Rx-LC</th>
<th>Rx-I</th>
<th>Tx-Domain</th>
<th>Tx-I</th>
</tr>
</thead>
<tbody>
<tr>
<td>1001</td>
<td>md1</td>
<td>1234567890</td>
<td>3001</td>
<td>Y</td>
<td>N</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Related Commands
None

13.3.51  show ethernet cfm lm brief

Command Purpose
Use the command to display all meps which are enabled loss measurement.

Command Syntax
show ethernet cfm lm brief

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following example shows how to display Im brief information:
Switch#  show ethernet cfm lm brief

------------------------------------------
MPID Domain VLAN LM-En
------------------------------------------
1  md1  2  dual-lm-enabled
5  md1  2  single-lm-enabled

Related Commands
None

13.3.52  ethernet cfm tst transmission enable

Command Purpose
Use this command to enable test transmission enable.

Command Syntax
ethernet cfm tst transmission enable session SESSION_ID domain DOMAIN_NAME ( vlan VLAN_ID | ) mep MEPID tx-mode ( fixed pkt-num NUMBER | continuous ) ( ( pattern-type ( repeat VALUE | random | increment-byte | decrement-byte ) | packet-size PACKET_SIZE | dest-mac ( multicast | MACADDRESS ) ) )
no ethernet cfm tst transmission enable session SESSION_ID domain DOMAIN_NAME ( vlan VLAN_ID | ) mepid MEPID
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SESSION_ID</td>
<td>session id</td>
<td>1-4</td>
</tr>
<tr>
<td>DOMAIN_NAME</td>
<td>Maintenance domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>vlan VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
<tr>
<td>MEPID</td>
<td>Local mep id</td>
<td>1-8191</td>
</tr>
<tr>
<td>NUMBER</td>
<td>Transmission packet number</td>
<td>1-65535</td>
</tr>
<tr>
<td>VALUE</td>
<td>The value of repeat pattern type, the range is 0 to 0xFFFFFFFF</td>
<td>0 - 0xFFFFFFFF</td>
</tr>
<tr>
<td>PACKET_SIZE</td>
<td>Transmission packet size, the range is 64 bytes to 16027 bytes, default is 512 bytes</td>
<td>64-16027 bytes</td>
</tr>
<tr>
<td>multicast</td>
<td>The destination mac address of tst packets should be multicast address, default is multicast</td>
<td>-</td>
</tr>
<tr>
<td>MACADDRESS</td>
<td>The destination mac address of tst packets should be unicast mac address</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

None

**Usage**

None

**Examples**

The following example shows how to enable maintenance domain tst for mep:

Switch# configure terminal

Switch(config)# ethernet cfm tst transmission enable domain md1 vlan 2 mepid 1 tx-mode continuous pattern-type random packet-size 1518

**Related Commands**

None

13.3.53 ethernet cfm tst start/stop

**Command Purpose**

Use this command to start or stop test transmission.

**Command Syntax**

```
ethernet cfm tst start session SESSION_ID rate RATE time ( cos COS_VALUE | ) ( second SECOND | 1m | 15m | 2h | 24h ) ( tx_port TX_PORT | )
ethernet cfm tst stop
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SESSION_ID</td>
<td>session id</td>
<td>1-4</td>
</tr>
<tr>
<td>RATE</td>
<td>Transmission rate, the range is 1 to 10000, unit is mbps</td>
<td>1-10000 mbps</td>
</tr>
<tr>
<td>cos COS_VALUE</td>
<td>Vlan priority, default value is 7</td>
<td>0-7</td>
</tr>
<tr>
<td>SECOND</td>
<td>Transmission time from 1 second to 60 seconds</td>
<td>1-60 seconds</td>
</tr>
<tr>
<td>15m</td>
<td>Transmission time for every rate is 15 minutes</td>
<td>-</td>
</tr>
<tr>
<td>2h</td>
<td>Transmission time for every rate is 2 hours</td>
<td>-</td>
</tr>
<tr>
<td>24h</td>
<td>Transmission time for every rate is 24 hours</td>
<td>-</td>
</tr>
<tr>
<td>TX_PORT</td>
<td>Transmission port, only valid for up mep</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
The following example shows how to start test transmission for mep:
```
Switch# configure terminal
Switch(config)# ethernet cfm tst start session 2 rate 10 time second 1
Switch# configure terminal
Switch(config)# ethernet cfm tst start time second 1
```

**Related Commands**
None

**13.3.54 ethernet cfm tst reception enable**

**Command Purpose**
Use this command to enable test packet reception.

**Command Syntax**
```
ethernet cfm tst reception enable session SESSION_ID domain DOMAIN_NAME (vlan VLAN_ID | ) mepid MEPID
no ethernet cfm tst reception enable session SESSION_ID domain DOMAIN_NAME (vlan VLAN_ID | ) mepid MEPID
```
### Command Mode

**Global Configuration**

**Default**

None

**Usage**

Test transmission and reception must be configured on the same MEP.

**Examples**

The following example shows how to enable test reception for mep:

```plaintext
Switch# configure terminal
Switch(config)# ethernet cfm tst reception enable session 1 domain md1 vlan 2 mep 1
Switch# configure terminal
Switch(config)# ethernet cfm tst reception enable domain md1 vlan 2 mepid 1
```

**Related Commands**

None

---

### show ethernet cfm tst

**Command Purpose**

Use the command to display test information.

**Command Syntax**

```
show ethernet cfm tst
```

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

The sending side test information:

```plaintext
Switch# show ethernet cfm tst

DOMAIN : md1
```

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>session</td>
<td>Session id</td>
<td>1-4</td>
</tr>
<tr>
<td>DOMAIN_NAME</td>
<td>Maintenance domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>vlan VLAN_ID</td>
<td>Vlan id</td>
<td>1-4094</td>
</tr>
<tr>
<td>MEPID</td>
<td>Local mep id</td>
<td>1-8191</td>
</tr>
</tbody>
</table>
VLAN : 2
MEPID : 2
Transmission : Disabled
Reception : Enabled
Status : Non-Running
Start Time : null
End Time : null
Packet Type : null
Rate : null
Packet Size : null
Tx Number : 0
Tx Bytes : 0
Rx Number : 28
Rx Bytes : 1792

Related Commands
None

13.3.56 clear ethernet cfm tst counters
Command Purpose
Use the command to clear test counters.

Command Syntax
clear ethernet cfm tst counters

Command Mode
Privileged EXEC

Default
None

Usage
When test transmission is running, can't clear ethernet cfm test counters.

Examples
The following example shows how to clear test counters:
$Switch# clear ethernet cfm tst counters

Related Commands
None

13.4 CPU Traffic Limit Commands

13.4.1 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 \textit{RATE\_RANGE}
no cpu-traffic-limit total rate

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>\textit{RATE_RANGE}</td>
<td>Rate of all streams destined to cpu in pps</td>
<td>0-1000000</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

2048 pps

Usage

N/A

Examples

This example shows how to configure cpu-traffic-limit total rate:

\texttt{Switch\# configure terminal}

\texttt{Switch(config)\# cpu-traffic-limit total rate 3000}

This example shows how to reset cpu-traffic-limit total rate:

\texttt{Switch\# configure terminal}

\texttt{Switch(config)\# no cpu-traffic-limit total rate}

Related Commands

\texttt{show cpu traffic-limit}

13.4.2 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-securitydiscard | vlan-security-discard | ip-mtu-fail | ip-option | ucast-ttl-fail | mpls-ttl-fail | igmp | sflow-ingress | fwd-to-cpu | udld | bfd-learning \} rate \textit{RATE\_RANGE}
no cpu-traffic-limit reason \{ bpdu | slow-protocol | eapol | erps | smart-link | arp | dhcp | rip | ldp | ospf | pim | vrrp | ipda | icmp-redirect | mcast-rpf-fail | macsa-mismatch | port-security-discard | vlan-security-discard | ip-mtu-fail | ip-option | ucast-ttl-fail | mpls-ttl-fail | igmp | sflow-ingress | sflow-egress | fwd-to-cpu | udld | bfd-learning \} rate

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>bpdu</td>
<td>Reason for BPDU protocols packets (including STP, RSTP, MSTP)</td>
<td>-</td>
</tr>
<tr>
<td>slow-protocol</td>
<td>Reason for slow protocol packets (including EFM, LACP)</td>
<td>-</td>
</tr>
<tr>
<td>eapol</td>
<td>Reason for Dot1x protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>Parameter</td>
<td>Parameter Description</td>
<td>Parameter Value</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>erps</td>
<td>Reason for ERPS protocol packets</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Reason for ERPS protocol packets</td>
<td></td>
</tr>
<tr>
<td>arp</td>
<td>Reason for ARP protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>dhcp</td>
<td>Reason for DHCP protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>rip</td>
<td>Reason for RIP protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>bgp</td>
<td>Reason for BGP protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>ldp</td>
<td>Reason for LDP protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>ospf</td>
<td>Reason for OSPF protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>pim</td>
<td>Reason for PIM protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>vrrp</td>
<td>Reason for VRRP protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>ssh</td>
<td>Reason for SSH protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>telnet</td>
<td>Reason for Telnet protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>mlag</td>
<td>Reason for MLAG protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>tcp</td>
<td>Reason for TCP protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>ipda</td>
<td>Reason for packets with IPDA destination to router itself</td>
<td>-</td>
</tr>
<tr>
<td>icmp-redirect</td>
<td>Reason for redirecting ICMP</td>
<td>-</td>
</tr>
<tr>
<td>learning-full</td>
<td>Reason for learning cache is full</td>
<td>-</td>
</tr>
<tr>
<td>mcast_rpf_fail</td>
<td>Reason for multi-cast packets with rpf fail</td>
<td>-</td>
</tr>
<tr>
<td>macsa-mismatch</td>
<td>Reason for packets that are discarded for source mac is learned from another security port</td>
<td>-</td>
</tr>
<tr>
<td>port-security-discard</td>
<td>Reason for packets that are discarded for fdb number equals to allowed maximum number of security port</td>
<td>-</td>
</tr>
<tr>
<td>vlan-security-discard</td>
<td>Reason for packets that are discarded for fdb number equals to allowed maximum number on the specified vlan</td>
<td>-</td>
</tr>
<tr>
<td>ip-mtu-fail</td>
<td>Ip mtu fail</td>
<td>-</td>
</tr>
<tr>
<td>Parameter</td>
<td>Parameter Description</td>
<td>Parameter Value</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Ip-option</td>
<td>Reason for IP packets with optional fields</td>
<td>-</td>
</tr>
<tr>
<td>ucast-ttl-fail</td>
<td>Reason for ucast ip packets with fail TTL</td>
<td>-</td>
</tr>
<tr>
<td>mpls-ttl-fail</td>
<td>Reason for mpls packets with fail TTL</td>
<td>-</td>
</tr>
<tr>
<td>Igmp</td>
<td>Reason for IGMP or igmp snooping packets</td>
<td>-</td>
</tr>
<tr>
<td>sflow-ingress</td>
<td>Reason for sflow sampled packets at ingress direction</td>
<td>-</td>
</tr>
<tr>
<td>sflow-egress</td>
<td>Reason for sflow sampled packets at egress direction</td>
<td>-</td>
</tr>
<tr>
<td>fwd-to-cpu</td>
<td>Reason for packets forwarding to cpu</td>
<td>-</td>
</tr>
<tr>
<td>bfd-learning</td>
<td>Reason for bfd learning packets</td>
<td>-</td>
</tr>
<tr>
<td>RATE_RANGE</td>
<td>Individual rate of streams destined to cpu carried with the reason in kbps</td>
<td>0-1000000</td>
</tr>
<tr>
<td>mld</td>
<td>mld packets or mld snooping packets</td>
<td>-</td>
</tr>
<tr>
<td>dot1x-mac-bypass</td>
<td>mac auth bypass packets</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

**Global Configuration**

**Default**

<table>
<thead>
<tr>
<th>Reason</th>
<th>Rate(pps)</th>
<th>Reason</th>
<th>Rate(pps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>bpdu</td>
<td>64</td>
<td>icmp-redirect</td>
<td>128</td>
</tr>
<tr>
<td>slow-protocol</td>
<td>128</td>
<td>mcast-rpf-fail</td>
<td>128</td>
</tr>
<tr>
<td>eapol</td>
<td>128</td>
<td>macsa-mismatch</td>
<td>128</td>
</tr>
<tr>
<td>erps</td>
<td>128</td>
<td>port-security-discard</td>
<td>128</td>
</tr>
<tr>
<td>smart-link</td>
<td>128</td>
<td>vlan-security-discard</td>
<td>128</td>
</tr>
<tr>
<td>arp</td>
<td>640</td>
<td>udld</td>
<td>128</td>
</tr>
<tr>
<td>dhcp</td>
<td>128</td>
<td>ip-mtu-fail</td>
<td>64</td>
</tr>
<tr>
<td>Reason</td>
<td>Rate(pps)</td>
<td>Reason</td>
<td>Rate(pps)</td>
</tr>
<tr>
<td>--------</td>
<td>-----------</td>
<td>--------</td>
<td>-----------</td>
</tr>
<tr>
<td>rip</td>
<td>64</td>
<td>fwd-to-cpu</td>
<td>64</td>
</tr>
<tr>
<td>ldp</td>
<td>512</td>
<td>ip-option</td>
<td>512</td>
</tr>
<tr>
<td>ospf</td>
<td>256</td>
<td>ucast-ttl-fail</td>
<td>64</td>
</tr>
<tr>
<td>pim</td>
<td>128</td>
<td>mpls-ttl-fail</td>
<td>64</td>
</tr>
<tr>
<td>vrrp</td>
<td>512</td>
<td>igmp</td>
<td>128</td>
</tr>
<tr>
<td>ssh</td>
<td>64</td>
<td>telnet</td>
<td>64</td>
</tr>
<tr>
<td>mlag</td>
<td>1024</td>
<td>tcp</td>
<td>64</td>
</tr>
<tr>
<td>ipda</td>
<td>1024</td>
<td>sflow-ingress</td>
<td>128</td>
</tr>
<tr>
<td>sflow-egress</td>
<td>128</td>
<td>bfd-learning</td>
<td>128</td>
</tr>
<tr>
<td>sflow-egress</td>
<td>128</td>
<td>bfd-learning</td>
<td>128</td>
</tr>
</tbody>
</table>

**Usage**

ssh/telnet/mlag is useful when enable cpu-traffic-optimize.

**Examples**

This example shows how to configure individual rate for BPDU PDU:

```
Switch# configure terminal
Switch(config)# cpu-traffic-limit reason bpdu rate 300
```

This example shows how to reset individual rate for BPDU PDU:

```
Switch# configure terminal
Switch(config)# no cpu-traffic-limit reason bpdu rate
```

**Related Commands**

show cpu traffic-limit

**13.4.3 cpu-traffic-limit reason class**

**Command Purpose**

Use this command to set the priority class for the stream carried with the reason. Use the no form of this command to set the priority class of the reason to its default value.

**Command Syntax**

```
cpu-traffic-limit reason { bpdu | slow-protocol | eapol | erps | smart-link | arp | dhcp | rip | ldp | ospf | pim | vrrp | ssh | telnet | mlag | tcp | ipda | icmp-redirect | mcast-rpf-fail | macsa-mismatch | port-security-discard | vlan-security-discard | mtu-dontfrag | mtu-frag | ip-option | ucast-ip-ttl-fail | mpls-ttl-fail | igmp | sflow-ingress | udld | bfd-learning | class CLASS_RANGE}
```

```
no cpu-traffic-limit reason { bpdu | slow-protocol | eapol | erps | smart-link | arp | dhcp | rip | ldp | ospf | pim | vrrp | ssh | telnet | mlag | tcp | ipda | icmp-redirect | mcast-rpf-fail | macsa-mismatch | port-security-discard | vlan-security-discard | mtu-dontfrag | mtu-frag | ip-option | ucast-ip-ttl-fail | mpls-ttl-fail | igmp | sflow-ingress | sflow-egress | udld | bfd-learning | class }
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLASS_RANGE</td>
<td>Priority of the stream carried with this reason. Reason with class 3 has the highest priority.</td>
<td>0-3</td>
</tr>
</tbody>
</table>
Command Mode

Global Configuration

Default

<table>
<thead>
<tr>
<th>Reason</th>
<th>class</th>
<th>Reason</th>
<th>class</th>
</tr>
</thead>
<tbody>
<tr>
<td>bpdu</td>
<td>3</td>
<td>icmp-redirect</td>
<td>0</td>
</tr>
<tr>
<td>slow-protocol</td>
<td>1</td>
<td>mcast-rpf-fail</td>
<td>1</td>
</tr>
<tr>
<td>eapol</td>
<td>0</td>
<td>macsa-mismatch</td>
<td>0</td>
</tr>
<tr>
<td>erps</td>
<td>2</td>
<td>port-securitydiscard</td>
<td>0</td>
</tr>
<tr>
<td>smart-link</td>
<td>2</td>
<td>vlan-security-discard</td>
<td>0</td>
</tr>
<tr>
<td>arp</td>
<td>1</td>
<td>udld</td>
<td>3</td>
</tr>
<tr>
<td>dhcp</td>
<td>0</td>
<td>mtu-dontfrag</td>
<td>0</td>
</tr>
<tr>
<td>rip</td>
<td>1</td>
<td>mtu-frag</td>
<td>0</td>
</tr>
<tr>
<td>ldp</td>
<td>1</td>
<td>sflow-ingress</td>
<td>0</td>
</tr>
<tr>
<td>ospf</td>
<td>1</td>
<td>ip-option</td>
<td>0</td>
</tr>
<tr>
<td>pim</td>
<td>1</td>
<td>ucast-ttl-fail</td>
<td>0</td>
</tr>
<tr>
<td>vrrp</td>
<td>1</td>
<td>mpls-ttl-fail</td>
<td>0</td>
</tr>
<tr>
<td>igmp</td>
<td>2</td>
<td>ssh</td>
<td>3</td>
</tr>
<tr>
<td>telnet</td>
<td>3</td>
<td>mlag</td>
<td>1</td>
</tr>
<tr>
<td>tcp</td>
<td>2</td>
<td>ipda</td>
<td>0</td>
</tr>
<tr>
<td>igmp</td>
<td>2</td>
<td>mld</td>
<td>2</td>
</tr>
<tr>
<td>sflow-egress</td>
<td>0</td>
<td>dot1x-mac-bypass</td>
<td>2</td>
</tr>
<tr>
<td>fwd-to-cpu</td>
<td>0</td>
<td>bfd-learning</td>
<td>1</td>
</tr>
<tr>
<td>fwd-to-cpu</td>
<td>0</td>
<td>bfd-learning</td>
<td>1</td>
</tr>
</tbody>
</table>

Usage

The reason with the highest priority class will get preference treatment when dealing with scheduling. ssh/telnet/mlag is useful when enable cpu-traffic-optimize.

Examples

This example shows how to configure priority class for BPDU:

Switch# configure terminal

Switch(config)# cpu-traffic-limit reason bpdu class 3

Related Commands

show cpu traffic-limit
13.4.4 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
```

<table>
<thead>
<tr>
<th>reason</th>
<th>rate (pps)</th>
<th>class</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x-mac-bypass</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>bpdu</td>
<td>64</td>
<td>3</td>
</tr>
<tr>
<td>slow-protocol</td>
<td>128</td>
<td>1</td>
</tr>
<tr>
<td>eapol</td>
<td>128</td>
<td>0</td>
</tr>
<tr>
<td>erps</td>
<td>128</td>
<td>2</td>
</tr>
<tr>
<td>smart-link</td>
<td>128</td>
<td>2</td>
</tr>
<tr>
<td>udld</td>
<td>128</td>
<td>3</td>
</tr>
<tr>
<td>loopback-detection</td>
<td>64</td>
<td>3</td>
</tr>
<tr>
<td>arp</td>
<td>256</td>
<td>1</td>
</tr>
<tr>
<td>dhcp</td>
<td>128</td>
<td>0</td>
</tr>
<tr>
<td>rip</td>
<td>64</td>
<td>1</td>
</tr>
<tr>
<td>ldp</td>
<td>512</td>
<td>1</td>
</tr>
<tr>
<td>ospf</td>
<td>256</td>
<td>1</td>
</tr>
<tr>
<td>pim</td>
<td>128</td>
<td>1</td>
</tr>
<tr>
<td>bgp</td>
<td>256</td>
<td>1</td>
</tr>
<tr>
<td>vrrp</td>
<td>512</td>
<td>1</td>
</tr>
<tr>
<td>rsvp</td>
<td>512</td>
<td>1</td>
</tr>
<tr>
<td>ssh</td>
<td>64</td>
<td>3</td>
</tr>
<tr>
<td>telnet</td>
<td>64</td>
<td>3</td>
</tr>
<tr>
<td>mlag</td>
<td>1024</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>64</td>
<td>2</td>
</tr>
<tr>
<td>ipda</td>
<td>1024</td>
<td>0</td>
</tr>
<tr>
<td>icmp-redirect</td>
<td>128</td>
<td>0</td>
</tr>
<tr>
<td>mcast-rpf-fail</td>
<td>128</td>
<td>1</td>
</tr>
<tr>
<td>macsa-mismatch</td>
<td>128</td>
<td>0</td>
</tr>
<tr>
<td>port-security-discard</td>
<td>128</td>
<td>0</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------</td>
<td>-----------------</td>
</tr>
<tr>
<td>vlan-security-discard</td>
<td>128</td>
<td></td>
</tr>
<tr>
<td>ip-mtu-fail</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>bfd-learning</td>
<td>128</td>
<td></td>
</tr>
<tr>
<td>ptp</td>
<td>512</td>
<td>2</td>
</tr>
<tr>
<td>ip-option</td>
<td>512</td>
<td>0</td>
</tr>
<tr>
<td>tunnel-gre-keepalive</td>
<td>64</td>
<td>0</td>
</tr>
<tr>
<td>ucast-ttl-fail</td>
<td>64</td>
<td>0</td>
</tr>
<tr>
<td>mpls-ttl-fail</td>
<td>64</td>
<td>0</td>
</tr>
<tr>
<td>igmp</td>
<td>128</td>
<td>2</td>
</tr>
<tr>
<td>sflow-ingress</td>
<td>128</td>
<td>0</td>
</tr>
<tr>
<td>sflow-egress</td>
<td>128</td>
<td>0</td>
</tr>
<tr>
<td>fwd-to-cpu</td>
<td>64</td>
<td>0</td>
</tr>
<tr>
<td>l2protocol-tunnel</td>
<td>1024</td>
<td>0</td>
</tr>
<tr>
<td>mirror-to-cpu</td>
<td>256</td>
<td>0</td>
</tr>
<tr>
<td>mpls-tp-pwoam</td>
<td>128</td>
<td>2</td>
</tr>
</tbody>
</table>

Total rate: 2048 (pps)

Related Commands

cpu-traffic-limit total rate
cpu-traffic-limit reason rate

13.5 CPU Traffic Statistics Commands

13.5.1 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RATE-TIME</td>
<td>Rate of statistics time</td>
<td>1-10 seconds</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

5 s

Usage

N/A

Examples

This example shows how to configure cpu-traffic-statistics time:

Switch# configure terminal
Switch(config)# cpu-traffic-statistics time 2
Related Commands
N/A

13.5.2 no cpu-traffic-statistics time

Command Purpose
Use this command to reset the CPU receive packets or CPU transmit packets statistics time.

Command Syntax
no cpu-traffic-statistics time

Command Mode
Global Configuration

Default
N/A

Usage
N/A

Examples
This example shows how to reset cpu-traffic-statistics time:
Switch# configure terminal
Switch(config)# no cpu-traffic-statistics time

Related Commands
N/A

13.5.3 show cpu-traffic-statistics receive

Command Purpose
Use this command to show CPU receive packets by reason.

Command Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>bpdu</td>
<td>Reason for BPDU protocols packets (including STP, RSTP, MSTP)</td>
<td>-</td>
</tr>
<tr>
<td>slow-protocol</td>
<td>Reason for slow protocol packets (including EFM, LACP)</td>
<td>-</td>
</tr>
<tr>
<td>eapol</td>
<td>Reason for Dot1x protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>erps</td>
<td>Reason for ERPS protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>arp</td>
<td>Reason for ARP protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>Parameter</td>
<td>Parameter Description</td>
<td>Parameter Value</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>dhcp</td>
<td>Reason for DHCP protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>rip</td>
<td>Reason for RIP protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>bgp</td>
<td>Reason for BGP protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>ldp</td>
<td>Reason for LDP protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>ospf</td>
<td>Reason for OSPF protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>pim</td>
<td>Reason for PIM protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>vrrp</td>
<td>Reason for VRRP protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>ssh</td>
<td>Reason for SSH protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>telnet</td>
<td>Reason for Telnet protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>mlag</td>
<td>Reason for MLAG protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>tcp</td>
<td>Reason for TCP protocol packets</td>
<td>-</td>
</tr>
<tr>
<td>ipda</td>
<td>Reason for packets with IPDA destination to router itself</td>
<td>-</td>
</tr>
<tr>
<td>icmp-redirect</td>
<td>Reason for redirecting ICMP</td>
<td>-</td>
</tr>
<tr>
<td>learning-full</td>
<td>Reason for learning cache is full</td>
<td>-</td>
</tr>
<tr>
<td>mcast_rpf_fail</td>
<td>Reason for multi-cast packets with rpf fail</td>
<td>-</td>
</tr>
<tr>
<td>macsa-mismatch</td>
<td>Reason for packets that are discarded for source mac is learned from another security port</td>
<td>-</td>
</tr>
<tr>
<td>port-security-discard</td>
<td>Reason for packets that are discarded forfdb number equals to allowed maximum number of security port</td>
<td>-</td>
</tr>
<tr>
<td>vlan-security-discard</td>
<td>Reason for packets that are discarded forfdb number equals to allowed maximum number on the specified vlan</td>
<td>-</td>
</tr>
<tr>
<td>ip-mtu-fail</td>
<td>Ip mtu fail</td>
<td>-</td>
</tr>
<tr>
<td>lp-option</td>
<td>Reason for IP packets with optional fields</td>
<td>-</td>
</tr>
<tr>
<td>ucast-ttl-fail</td>
<td>Reason for ucast ip packets with fail ttl</td>
<td>-</td>
</tr>
<tr>
<td>Parameter</td>
<td>Parameter Description</td>
<td>Parameter Value</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>mpls-ttl-fail</td>
<td>Reason for mpls packets with fail</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TTL</td>
<td></td>
</tr>
<tr>
<td>igmp</td>
<td>Reason for IGMP or igmp snooping packets</td>
<td></td>
</tr>
<tr>
<td>sflow-ingress</td>
<td>Reason for sflow sampled packets at ingress direction</td>
<td></td>
</tr>
<tr>
<td>sflow-egress</td>
<td>Reason for sflow sampled packets at egress direction</td>
<td></td>
</tr>
<tr>
<td>fwd-to-cpu</td>
<td>Reason for packets forwarding to cpu</td>
<td></td>
</tr>
<tr>
<td>bfd-learning</td>
<td>Reason for bfd learning packets</td>
<td></td>
</tr>
<tr>
<td>mld</td>
<td>mld packets or mld snooping packets</td>
<td></td>
</tr>
<tr>
<td>dot1x-mac-bypass</td>
<td>mac auth bypass packets</td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>statistics rate time is 5 second(s)</th>
<th>reason</th>
<th>count(packets)</th>
<th>rate(pps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>bpdu</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Related Commands**

show cpu traffic-statistics receive all

**13.5.4 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

<table>
<thead>
<tr>
<th>reason</th>
<th>count(packets)</th>
<th>rate(pps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x-mac-bypass</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>bpdu</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>slow-protocol</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>eapol</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>erps</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>smart-link</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>udld</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>loopback-detection</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>arp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dhcp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>rip</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ldp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ospf</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>pim</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>bgp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>vrrp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>rsvp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ssh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>telnet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>mlag</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ipda</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>icmp-redirect</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>mcast-rpf-fail</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>macsa-mismatch</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>port-security-discard</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>vlan-security-discard</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ip-mtu-fail</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>bfd-learning</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ptp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ip-option</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Related Commands

N/A

13.5.5 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

<table>
<thead>
<tr>
<th></th>
<th>count(packets)</th>
<th>rate(pps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>statistics rate time is 5 second(s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Related Commands
N/A
13.6 CPU Traffic Protect Commands

13.6.1 cpu-traffic-protect arp

Command Purpose
Use this command to enable and enter into arp protect mode. Use the no form of this command to disable arp protect mode.

Command Syntax
cpu-traffic-protect arp
no cpu-traffic-protect arp

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>arp</td>
<td>ARP packet</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
Enter into blacklist mode after enable

Examples
This example shows how to enable and enter into arp protect mode:
Switch# configure terminal
Switch(config)# cpu-traffic-protect arp
Switch(config-cpu-traffic-protect)#

Related Commands
N/A

13.6.2 trace enable

Command Purpose
Use this command to enable attack trace. Use the no form of this command to disable attack trace.

Command Syntax
trace enable
no trace enable

Command Mode
Cpu traffic Protect Configuration

Default
None

Usage
None
Examples

This example shows how to enable attack trace:
Switch# configure terminal
Switch(config-cpu-traffic-protect)# trace enable

Related Commands

N/A

13.6.3 trace type

Command Purpose

Use this command to configure attack trace type. Use the no form of this command to set to the default type.

Command Syntax

trace type (sender-ip | src-mac | target-ip | source-portvlan)
no trace type

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>sender-ip</td>
<td>ARP packet sender ip address</td>
<td>-</td>
</tr>
<tr>
<td>src-mac</td>
<td>ARP packet source MAC</td>
<td>-</td>
</tr>
<tr>
<td>target-ip</td>
<td>ARP packet target ip address</td>
<td>-</td>
</tr>
<tr>
<td>source-portvlan</td>
<td>The port and vlan packet input</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Cpu traffic Protect Configuration

Default

src-mac

Usage

None

Examples

This example shows how to configure attack trace type to sender-ip and target-ip:
Switch# configure terminal
Switch(config-cpu-traffic-protect)# trace type sender-ip target-ip

Related Commands

N/A

13.6.4 trace sample

Command Purpose

Use this command to configure attack trace sample rate. Use the no form of this command to set sample to the default.

Command Syntax

trace sample SAMPLE-RATE
no trace sample
### SAMPLE-RATE

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAMPLE-RATE</td>
<td>Attack trace sample rate</td>
<td>1-1024</td>
</tr>
</tbody>
</table>

#### Command Mode

Cpu traffic Protect Configuration

#### Default

8

#### Usage

None

#### Examples

This example shows how to configure attack trace sample rate to 16:

Switch# configure terminal

Switch(config-cpu-traffic-protect)# trace sample 16

### Related Commands

#### 13.6.5 trace threshold

#### Command Purpose

Use this command to configure attack trace checking threshold. Use the no form of this command to set threshold to the default.

#### Command Syntax

```
trace threshold THRESHOLD
no trace threshold
```

### Command Mode

Cpu traffic Protect Configuration

#### Default

128

#### Usage

None

#### Examples

This example shows how to configure attack trace checking threshold to 10:

Switch# configure terminal

Switch(config-cpu-traffic-protect)# trace threshold 10

### Related Commands
13.6.6 apply access-list

Command Purpose
Use this command to configure arp protect filter rules. Use the no form of this command to disable rules.

Command Syntax
apply access-list NAME (mode (blacklist | whitelist (rate RATE | |)))
no apply access-list ACL-NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL-NAME</td>
<td>Extend ip access list name</td>
<td>-</td>
</tr>
<tr>
<td>blacklist</td>
<td>Blacklist mode</td>
<td>-</td>
</tr>
<tr>
<td>whitelist</td>
<td>Whitelist mode</td>
<td>-</td>
</tr>
<tr>
<td>RATE</td>
<td>Packet to cpu rate</td>
<td>32-2048,unit:pps</td>
</tr>
</tbody>
</table>

Command Mode
Cpu traffic Protect Configuration

Default
Rate: 32pps, Mode: blacklist

Usage
The rate is calculated by using 64 Btyes packet

Examples
This example shows how to configure arp protect filter rules with access list 2 and enter into whitelist mode and the rate is 64pps:
Switch# configure terminal
Switch(config-cpu-traffic-protect)# apply access-list 2 mode whitelist rate 64

Related Commands

13.6.7 show cpu traffic-protect trace

Command Purpose
Use this command to show the information of attack trace.

Command Syntax
show cpu traffic-protect trace (history | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>history</td>
<td>History trace information</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None
Usage

None

Examples

This example shows how to show the information of attack trace:
Switch# show cpu traffic-protect trace

<table>
<thead>
<tr>
<th>MacAddress</th>
<th>Interface</th>
<th>Vlan/O/I</th>
<th>AttackTime</th>
<th>TotalPackets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.0b00.0200</td>
<td>eth-0-3</td>
<td>-</td>
<td>2019-01-02 15:18:21</td>
<td>1712</td>
</tr>
</tbody>
</table>

Total: 1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Vlan/O/I</th>
<th>AttackTime</th>
<th>TotalPackets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total: 0

<table>
<thead>
<tr>
<th>IPAddress</th>
<th>AttackTime</th>
<th>TotalPackets</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.3.4</td>
<td>2019-01-02 15:21:24</td>
<td>184</td>
</tr>
</tbody>
</table>

Total: 1

<table>
<thead>
<tr>
<th>IPAddress</th>
<th>AttackTime</th>
<th>TotalPackets</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.2.1</td>
<td>2019-01-02 15:21:24</td>
<td>184</td>
</tr>
</tbody>
</table>

Total: 1

Related Commands

clear cpu traffic-protect trace

13.6.8  show resource cpu traffic-protect

Command Purpose

Use this command to show the information of resource used.
Command Syntax
show resource cpu traffic-protect

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to show the information of resource used:
Switch# show resource cpu traffic-protect

<table>
<thead>
<tr>
<th>Resource</th>
<th>Used</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACEs</td>
<td>3</td>
<td>200</td>
</tr>
</tbody>
</table>

Related Commands
show resource qos

13.6.9 clear cpu traffic-protect trace

Command Purpose
Use this command to clear the information of attack trace.

Command Syntax
clear cpu traffic-protect trace ( type ( sender-ip | src-mac | target-ip | source-portvlan ) )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>sender-ip</td>
<td>ARP packet sender ip address</td>
<td>-</td>
</tr>
<tr>
<td>src-mac</td>
<td>ARP packet source MAC</td>
<td>-</td>
</tr>
<tr>
<td>target-ip</td>
<td>ARP packet target ip address</td>
<td>-</td>
</tr>
<tr>
<td>source-portvlan</td>
<td>The port and vlan packet input</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None
Examples

This example shows how to clear the information of attack trace:
Switch# clear cpu traffic-protect trace

Related Commands

13.6.10 clear cpu traffic-protect trace history

Command Purpose

Use this command to clear the history information of attack trace.

Command Syntax

clear cpu traffic-protect trace history

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>histroy</td>
<td>History trace information</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to clear the history information of attack trace:
Switch# clear cpu traffic-protect trace history

Related Commands

13.7 G.8031 Commands

13.7.1 g8031 eps-id

Command Purpose

Use this command to enter the eps configuration mode.
If the g8031 eps group with the specified eps-id does not exist, system will create a new one.
Use the no form of this command to delete the g8031 eps group.

Command Syntax

g8031 eps-id EPS_ID ( working-port IFNAME-W protection-port IFNAME-P | )
no g8031 eps-id EPS_ID

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>eps-id EPS_ID</td>
<td>unique id to identify an EPS protection link (1-2048)</td>
<td>1-2048</td>
</tr>
<tr>
<td>working-port IFNAME-W</td>
<td>interface name for working port</td>
<td>Support physical ports</td>
</tr>
<tr>
<td>protection-port IFNAME-P</td>
<td>interface name for protection port</td>
<td>Support physical ports</td>
</tr>
</tbody>
</table>
Command Mode
Global Configuration

Default
None

Usage
Use this command to enter the eps configuration mode.
If the g8031 eps group with the specified eps-id does not exist, system will create a new one. User should specify the working port and protection port when creating a group. The working port and protection port is not allowed to change after the eps group created.
If the g8031 eps group with the specified eps-id exists, user can enter the eps configuration mode without specify the working port and protection port.

Examples
The following example shows how to create a g8031 eps group and enter the eps configuration mode:
Switch# configure terminal
Switch(config)# g8031 eps-id 10 working-port eth-0-9 protection-port eth-0-10

Related Commands
instance
domain
show g8031

13.7.2 instance
Command Purpose
Use this command to bind an instance in a g8031 eps group.
Use the no form of this command to unbind the protected instance.

Command Syntax
instance INSTANCE_ID
no instance INSTANCE_ID

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE_ID</td>
<td>Set restrictions for the port of particular instance</td>
<td>0-4094</td>
</tr>
</tbody>
</table>

Command Mode
EPS Configuration

Default
None

Usage
Use this command to bind an instance in g8032 ring. The instance should exist in the mstp config mode before binding.
User can bind more than one instance in a g8032 ring.

Examples
The following example shows how to bind an instance in g8031 eps group:
Switch# configure terminal
Switch(g8031-config-switching)# instance 10

Related Commands
g8031 eps-id
show g8031
13.7.3 domain

Command Purpose

Use this command to bind a cfm maintains domain in the g8031 eps group. Use the no form of this command to unbind the cfm maintains domain.

Command Syntax

domain MD_NAME working-service MA_NAME_W protection-service MA_NAME_P
no domain

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain MD_NAME</td>
<td>maintenance-domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>working-service MA_NAME_W</td>
<td>maintenance-association name for working path</td>
<td>MD(Maintenance domain) name and MA(Maintenance association) name totally up to 44 characters.</td>
</tr>
<tr>
<td>protection-service MA_NAME_P</td>
<td>maintenance-association name for protection path</td>
<td>MD(Maintenance domain) name and MA(Maintenance association) name totally up to 44 characters.</td>
</tr>
</tbody>
</table>

Command Mode

EPS Configuration

Default
None

Usage

Use this command to bind a cfm maintains domain and maintains association in the g8032 ring. The cfm maintains domain and maintains association should exist in the cfm configuration.

Examples

The following example shows how to bind a cfm maintains domain:

Switch# configure terminal
Switch(g8031-config-switching)# domain test working-service test1 protection-service test2

Related Commands
g8031 eps-id
show g8031

13.7.4 mode

Command Purpose

Use this command to set the mode of g8031 ethernet protection. Use the no form of this command to return to the default setting.

Command Syntax

g8031 mode (revertive | non-revertive)
no mode

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>revertive</td>
<td>Revertive mode</td>
<td>-</td>
</tr>
<tr>
<td>non-revertive</td>
<td>Non-revertive mode</td>
<td>-</td>
</tr>
</tbody>
</table>
**Command Mode**

EPS Configuration

**Default**

The default setting should be revertive mode.

**Usage**

Use this command to set the mode of g8031 ethernet protection.
After set the mode of g8031 ethernet protection, the state machine of APS should restart.

**Examples**

The following example shows how to change the mode of a g8031 eps group:
```
Switch# configure terminal
Switch(g8031-config-switching)# mode non-revertive
```

**Related Commands**

- g8031 eps-id
- show g8031

---

**13.7.5 timer**

**Command Purpose**

Use this command to set the hold-off timer or wait-to-restore timer of a g8031 ethernet protection group.
Use the no form of this command to return to the default setting.

**Command Syntax**

```
timer ( wait-to-restore TIME-VALUE | hold-off TIME-VALUE )
nor timer ( wait-to-restore | hold-off )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>wait-to-restore TIME-VALUE</td>
<td>EPS wait-to-restore timer(5-12min)</td>
<td>5-12 minutes</td>
</tr>
<tr>
<td>hold-off TIME-VALUE</td>
<td>EPS hold-off timer(0-100 in steps of 100ms)</td>
<td>0-100 in steps of 100ms</td>
</tr>
</tbody>
</table>

**Command Mode**

EPS Configuration

**Default**

The default value of wait-to-restore (WTR) period is 5 minutes.
The default value of hold-off timer is 0.
The default value of guard timer is 500ms.

**Usage**

Use this command to set the wait-to-restore timer or hold-off timer or guard-timer of g8032 ring.
The wait-to-restore (WTR) period, may be configured by the operator in 1 minute steps between 5 and 12 minutes; the default value is 5 minutes.
The range of the hold-off timer is 0 to 10 seconds in steps of 100 ms.
The guard timer may be configured by the operator in 100ms steps between 100ms and 2 seconds, with a default value of 500ms.

**Examples**

The following example shows how to change the timer of a g8031 eps group:
Switch# configure terminal
Switch(g8031-config-switching)# timer wait-to-restore 8
Switch(g8031-config-switching)# timer hold-off 5

Related Commands
g8031 eps-id
show g8031

13.7.6 g8031 force

Command Purpose
Use this command to trigger the local force-switch event of a g8031 ethernet protection group.

Command Syntax
g8031 force eps-id EPS_ID

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>eps-id EPS_ID</td>
<td>unique id to identify an EPS protection link</td>
<td>1-2048</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
Use this command to trigger the local force-switch event of a g8031 ethernet protection group. When the current state has the higher priority than force-switch, system should reject the operation.

Examples
The following example shows how to trigger the local force-switch event of a g8031 eps group:
Switch# g8031 force eps-id 10

Related Commands
g8031 eps-id
show g8031

13.7.7 g8031 manual

Command Purpose
Use this command to trigger the local manual-switch event of a g8031 ethernet protection group.

Command Syntax
g8031 manual eps-id EPS_ID

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>eps-id EPS_ID</td>
<td>unique id to identify an EPS protection link</td>
<td>1-2048</td>
</tr>
</tbody>
</table>
Command Mode

Privileged EXEC

Default

N/A

Usage

Use this command to trigger the local manual-switch event of a g8031 ethernet protection group. When the current state has the higher priority than manual-switch, system should reject the operation.

Examples

The following example shows how to trigger the local manual-switch event of a g8031 eps group:

Switch# g8031 manual eps-id 10

Related Commands

g8031 eps-id
show g8031

13.7.8 g8031 lockout

Command Purpose

Use this command to trigger the local lockout event of a g8031 ethernet protection group.

Command Syntax

g8031 lockout eps-id EPS_ID

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>eps-id EPS_ID</td>
<td>unique id to identify an EPS protection link</td>
<td>1-2048</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

N/A

Usage

Use this command to trigger the local lockout event of a g8031 ethernet protection group.

Examples

The following example shows how to trigger the local lockout event of a g8031 eps group:

Switch# g8031 lockout eps-id 10

Related Commands

g8031 eps-id
show g8031
13.7.9 g8031 exercise

Command Purpose
Use this command to trigger the local exercise event of a g8031 ethernet protection group.

Command Syntax

```
g8031 exercise eps-id EPS_ID
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>eps-id EPS_ID</td>
<td>unique id to identify an EPS protection link</td>
<td>1-2048</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
N/A

Usage
Use this command to trigger the local exercise event of a g8031 ethernet protection group.

Examples

The following example shows how to trigger the local exercise event of a g8031 eps group:

```
Switch# g8031 exercise eps-id 10
```

Related Commands

- g8031 eps-id
- show g8031

13.7.10 g8031 clear

Command Purpose
Use this command to trigger the local clear event of a g8031 ethernet protection group.

Command Syntax

```
g8031 clear eps-id EPS_ID
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>eps-id EPS_ID</td>
<td>unique id to identify an EPS protection link</td>
<td>1-2048</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
Use this command to trigger clear local event of a g8031 ethernet protection group.
Examples
The following example shows how to trigger clear local event of a g8031 eps group:
Switch# g8031 clear eps-id 10

Related Commands
show g8031
show g8031 eps-id

13.7.11 show g8031

Command Purpose
Use this command to show the configuration and statues of g8031 ethernet protection groups.

Command Syntax
show g8031 (eps-id EPS_ID |)

Parameter | Parameter Description | Parameter Value
----------|-----------------------|-----------------
eps-id EPS_ID | unique id to identify an EPS protection link | 1-2048

Command Mode
Privileged EXEC

Default
None

Usage
Use this command to show the configuration and statues of g8031 ethernet protection groups. User can enter the eps-id to show the specified group. If the eps-id is not specified, all groups should be shown.

Examples
The following example shows the result of using this command:
Switch# show g8031

Codes: ID - Group id of G.8031
       IF-W - Interface of working entity, IF-P - Interface of protection entity
       MD - Maintenance domain
       MA-W - Maintenance association of working entity
       MA-P - Maintenance association of protection entity
       CS - Current state, LS - Last state, LE - Last event, FS - Far end state
       R/B - Request signal & bridged signal, MODE - Revertive or Non-revertive
       WTR - Wait to restore, DFOP - Failure of protocol defects

<table>
<thead>
<tr>
<th>ID</th>
<th>IF-W</th>
<th>IF-P</th>
<th>MD</th>
<th>MA-W</th>
<th>MA-P</th>
<th>CS</th>
<th>LS</th>
<th>LE</th>
<th>FS</th>
<th>R/B</th>
<th>MODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>eth-0-9</td>
<td>eth-0-10</td>
<td>test</td>
<td>test1</td>
<td>test2</td>
<td>NR</td>
<td>NR</td>
<td>NR</td>
<td>NR</td>
<td>null</td>
<td>REV</td>
</tr>
</tbody>
</table>
APS Vid - 11
Active-Path - Working
DFOP State - Not in defect mode
Protected Instance - 10

---

**Related Commands**

g8031 eps-id

**13.7.12 debug g8031**

**Command Purpose**

Use this command to enable the debug of g8031 module. Use the no form of this command to disable the debug.

**Command Syntax**

db**ug g8031 (rx | tx | event | all)**

no debug g8031 (rx | tx | event | all)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>rx</td>
<td>Enable rx debugs</td>
<td>-</td>
</tr>
<tr>
<td>tx</td>
<td>Enable tx debugs</td>
<td>-</td>
</tr>
<tr>
<td>event</td>
<td>Enable event debugs</td>
<td>-</td>
</tr>
<tr>
<td>all</td>
<td>Enable all debugs</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

Use this command to enable the debug of g8031 module.

**Examples**

The following example shows how to enable the debug of g8031 module:

Switch# debug g8031 all
Switch# terminal monitor

**Related Commands**

None

---

**13.8 G.8032 Commands**

**13.8.1 g8032 ring-id**

**Command Purpose**

Use this command to enter the g8032 configuration mode. If the g8032 ring with the specified ring-id does not exist, system will create a new one. Use the no form of this command to delete the g8032 ring.
Command Syntax

g8032 ring-id RING_ID \( (\text{east-interface IFNAME-E west-interface IFNAME-W (is-sub-ring \(|\) |)} \)\)
g8032 ring-id RING_ID \( (\text{interface IFNAME major-ring-id MAJOR_RING_ID}) \)\)
no g8032 ring-id RING_ID

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ring-id RING_ID</td>
<td>unique id to identify an g8032 ring</td>
<td>1-2048</td>
</tr>
<tr>
<td>east-interface IFNAME-E</td>
<td>interface name for east interface Support physical ports</td>
<td></td>
</tr>
<tr>
<td>west-interface IFNAME-W</td>
<td>interface name for west interface  Support physical ports</td>
<td></td>
</tr>
<tr>
<td>interface IFNAME</td>
<td>interface name for sub-ring interface Support physical ports</td>
<td></td>
</tr>
<tr>
<td>major-ring-id MAJOR_RING_ID</td>
<td>unique id to identify an ethernet major-ring protection</td>
<td>1-2048</td>
</tr>
<tr>
<td>is-sub-ring</td>
<td>specify the ring as sub-ring</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
Use this command to enter the g8032 configuration mode.
If the g8032 ring with the specified ring-id does not exist, system will create a new one. User should specify the east interface and west interface when creating a group. The east interface and west interface is not allowed to change after the g8032 ring created.
If the g8032 ring with the specified ring-id exists, user can enter the g8032 configuration mode without specify the east interface and west interface.

Examples
The following example shows how to create a g8032 ring and enter the g8032 configuration mode:
```
Switch# configure terminal
Switch(config)# g8032 ring-id 1 east-interface eth-0-1 west-interface eth-0-2
Switch(g8032-config-switch)# exit
```
The following example shows how to create a g8032 sub ring and enter the g8032 configuration mode:
```
Switch# configure terminal
Switch(config)# g8032 ring-id 2 interface eth-0-3 major-ring-id 1
Switch(g8032-config-switch)# exit
```
The following example shows how to enter the g8032 configuration mode:
```
Switch# configure terminal
Switch(config)# g8032 ring-id 1
Switch(g8032-config-switch)# exit
Switch(config)# g8032 ring-id 2
Switch(g8032-config-switch)#
```

Related Commands
domain instance timer show g8032

www.fs.com
13.8.2 instance

Command Purpose

Use this command to bind an instance in g8032 ring. Use the no form of this command to unbind the instance.

Command Syntax

```
instance INSTANCE_ID
no instance INSTANCE_ID
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE_ID</td>
<td>Set restrictions for the port of particular instance</td>
<td>0-4094</td>
</tr>
</tbody>
</table>

Command Mode

G8032 Configuration

Default

None

Usage

Use this command to bind an instance in g8032 ring. The instance should exist in the mstp config mode before binding. User can bind more than one instance in a g8032 ring.

Examples

The following example shows how to bind an instance in g8032 ring:

```
Switch# configure terminal
Switch(g8032-config-switch)# instance 1
Switch(g8032-config-switch)#
```

Related Commands

domain
timer
show g8032

13.8.3 domain

Command Purpose

Use this command to bind a cfm maintains domain in the g8032 ring. Use the no form of this command to unbind the cfm maintains domain.

Command Syntax

```
domain MD_NAME service MA_NAME
no domain
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD_NAME</td>
<td>maintenance-domain name</td>
<td>String with up to 43 characters</td>
</tr>
<tr>
<td>MA_NAME</td>
<td>maintenance-association name</td>
<td>MD(Maintenance domain) name and MA(Maintenance association) name totally up to 44 characters.</td>
</tr>
</tbody>
</table>
Command Mode
G8032 Configuration

Default
None

Usage
Use this command to bind a cfm maintains domain and maintains association in the g8032 ring. The cfm maintains domain and maintains association should exist in the cfm configuration.

Examples
The following example shows how to bind a cfm maintains domain:
Switch# configure terminal
Switch(g8032-config-switch)# domain md1 service ma1
Switch(g8032-config-switch)#

Related Commands
instance
timer
show g8032

13.8.4 control-vlan

Command Purpose
Use this command to set the R-APS vlan of a g8032 ring. Use the no form of this command to delete the ring's R-APS vlan.

Command Syntax
control-vlan VID ( sub-ring )
no control-vlan

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VID</td>
<td>R-APS channel vlan id</td>
<td>2-4094</td>
</tr>
<tr>
<td>sub-ring</td>
<td>Sub-ring's R-APS channel</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
G8032 Configuration

Default
None

Usage
Use this command to set the R-APS channel vlan of a g8032 ring. R-APS messages should use a dedicated vlan. Notice that "a dedicated vlan" means learning is disabled for this vlan. Dynamic FDB is flushed and static FDB is deleted. User can not config static FDB for this vlan after is configured as a control vlan.

Examples
The following example shows how to set R-APS channel vlan:
Switch# configure terminal
Switch(g8032-config-switch)# control-vlan 22
Switch(g8032-config-switch)#
Related Commands

domain
instance
timer
show g8032

13.8.5 rpl owner

Command Purpose
Use this command to set the rpl of a g8032 ring.
Use the no form of this command to delete the rpl.

Command Syntax
rpl owner (EAST-INTERFACE | WEST-INTERFACE)
no rpl owner

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAST-INTERFACE</td>
<td>ring's east interface</td>
<td>-</td>
</tr>
<tr>
<td>WEST-INTERFACE</td>
<td>ring's west interface</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
G8032 Configuration

Default
None

Usage
Use this command to set the rpl of a g8032 ring. In a (major) ring, user can specify east interface or west interface as rpl, but User can only specify east-interface as rpl interface in a sub-ring.

Examples
The following example shows how to set rpl of a g8032 ring:

```
Switch# configure terminal
Switch(g8032-config-switch)# rpl owner east-interface
Switch(g8032-config-switch)#
```

Related Commands

domain
instance
timer
show g8032

13.8.6 timer

Command Purpose
Use this command to set the wait-to-restore timer or hold-off timer or guard-timer of a g8032 ring.
Use the no form of this command to return to the default setting.

Command Syntax

```
timer ( wait-to-restore TIMEVAL | hold-off TIMEVAL | guard-timer TIMEVAL )
no timer ( wait-to-restore | hold-off | guard-timer )
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>wait-to-restore</td>
<td>TIMEVAL g8032 wait-to-restore timer(5-12min)</td>
<td>5-12 minute</td>
</tr>
<tr>
<td>hold-off</td>
<td>TIMEVAL g8032 hold-off timer(0-10s)</td>
<td>0-10000 in multiple of 100ms</td>
</tr>
<tr>
<td>guard-timer</td>
<td>TIMEVAL g8032 guard timer(100ms-2s)</td>
<td>0-2000 in multiple of 100ms</td>
</tr>
</tbody>
</table>

**Command Mode**

G8032 Configuration

**Default**

The default value of wait-to-restore (WTR) period is 5 minutes.
The default value of hold-off timer is 0.
The default value of guard timer is 500ms.

**Usage**

Use this command to set the wait-to-restore timer or hold-off timer or guard-timer of g8032 ring.
The wait-to-restore (WTR) period, may be configured by the operator in 1 minute steps between 5 and 12 minutes; the default value is 5 minutes.
The range of the hold-off timer is 0 to 10 seconds in steps of 100 ms.
The guard timer may be configured by the operator in 100ms steps between 100ms and 2 seconds, with a default value of 500ms.

**Examples**

The following example shows how to change the wait-to-restore timer of a g8032 ring:
```
Switch# configure terminal
Switch(g8032-config-switch)# timer wait-to-restore 6
```

The following example shows how to change the hold-off timer of a g8032 ring:
```
Switch# configure terminal
Switch(g8032-config-switch)# timer hold-off 100
```

The following example shows how to change the guard timer of a g8032 ring:
```
Switch# configure terminal
Switch(g8032-config-switch)# timer guard-timer 200
```

**Related Commands**

domain
instance
show g8032

13.8.7  ring enable

**Command Purpose**

Use this command to start the g8032 ring state machine.

**Command Syntax**

ring enable

**Command Mode**

G8032 Configuration

**Default**

None
Usage

Use this command to start the g8032 ring state machine. The ring should have bind md/ma and instance before enable the ring.

Examples

The following example shows how to enable the ring:

```
Switch# configure terminal
Switch(g8032-config-switch)# ring enable
Switch(g8032-config-switch)#
```

Related Commands

- ring disable
- show g8032

13.8.8  ring disable

Command Purpose

Use this command to stop the g8032 ring state machine.

Command Syntax

```
ring disable
```

Command Mode

G8032 Configuration

Default

None

Usage

Use this command to stop the g8032 ring state machine.

Examples

The following example shows how to disable a g8032 ring:

```
Switch# configure terminal
Switch(g8032-config-switch)# ring disable
Switch(g8032-config-switch)#
```

Related Commands

- ring enable
- show g8032

13.8.9  show g8032

Command Purpose

Use this command to show the configuration and statues of g8032 ring.

Command Syntax

```
show g8032 ( ring-id RING_ID | interface IF_NAME )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RING_ID</td>
<td>unique id to identify an g8032 ring</td>
<td>1-2048</td>
</tr>
<tr>
<td>IF_NAME</td>
<td>interface name of g8032 ring</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None
Usage

Use this command to show the configuration and statues of g8032 ring.
User can enter the ring-id to show the specified ring. If the ring-id is not specified, all rings should be shown.

Examples

The following example shows the result of using this command:
Switch# show g8032

<table>
<thead>
<tr>
<th>RingID</th>
<th>MajorRing</th>
<th>State</th>
<th>East</th>
<th>Status</th>
<th>West</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>N/A</td>
<td>Idle</td>
<td>eth-0-9</td>
<td>Blocked</td>
<td>eth-0-13</td>
<td>Forward</td>
</tr>
</tbody>
</table>

Control Vlan : 4094
MD Name : md1
Service Id : ma1
Is Enabled : Yes
Mode : Revertive
Node Role : Owner
Is Sub_ring : No
Protect Instance : 1-2
RPL : east-interface
Wait-to-restore : 05:00
Hold-off Timer : 0 (msecs)
Guard Timer : 500 (msecs)
WTB Timer : 5500 (msecs)
RAPS MEL : 7
Is Forward-to-cpu : 1

The following example shows the information of g8032 interface:
Switch# show g8032 interface eth-0-1

Interface State : Up

Ring ID : 1
Flush Logic

Remote Node ID : 92d5.b22e.cc00
Remote BPR : 0

Related Commands

- g8032 ring-id

13.8.10 debug g8032

Command Purpose

Use this command to enable the debug of g8032 module.
Use the no form of this command to disable the debug.
Command Syntax

default g8032 (rx | tx | event | all)
no default g8032 (rx | tx | event | all)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>rx</td>
<td>Enable rx debugs</td>
<td>-</td>
</tr>
<tr>
<td>tx</td>
<td>Enable tx debugs</td>
<td>-</td>
</tr>
<tr>
<td>event</td>
<td>Enable event debugs</td>
<td>-</td>
</tr>
<tr>
<td>all</td>
<td>Enable all debugs</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to enable the debug of g8032 module.

Examples

The following example shows how to enable the debug of g8032 module:

Switch# debug g8032 all
Switch# terminal monitor

Related Commands

None

13.8.11 g8032 force

Command Purpose

Use this command to trigger the local force-switch event of a g8032 ring port.

Command Syntax

g8032 force ring-id RING_ID (east-interface | west-interface)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RING_ID</td>
<td>Unique id to identify an g8032 ring</td>
<td>1-2048</td>
</tr>
<tr>
<td>east-interface</td>
<td>Trigger ring's east interface force-switch</td>
<td>-</td>
</tr>
<tr>
<td>west-interface</td>
<td>Trigger ring's west interface force-switch</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None
Usage
None

Examples
The following example shows how to g8032 force switch:
Switch# g8032 force ring-id 1 east-interface

Related Commands
show g8032

13.8.12  g8032 manual
Command Purpose
Use this command to trigger the local manual-switch event of a g8032 ring port.

Command Syntax
g8032 manual ring-id RING_ID ( east-interface | west-interface )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RING_ID</td>
<td>Unique id to identify an g8032 ring</td>
<td>1-2048</td>
</tr>
<tr>
<td>east-interface</td>
<td>Trigger ring's east interface manual-switch</td>
<td>-</td>
</tr>
<tr>
<td>west-interface</td>
<td>Trigger ring's west interface manual-switch</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following example shows how to g8032 manual switch:
Switch# g8032 manual ring-id 1 east-interface

Related Commands
show g8032

13.8.13  g8032 clear
Command Purpose
Use this command to clear the local force-switch or manual-switch of a g8032 ring port.

Command Syntax
g8032 clear ring-id RING_ID
### Command Mode

**Privileged EXEC**

### Default

None

### Usage

None

### Examples

The following example shows how to g8032 clear switch:

```
Switch# g8032 clear ring-id 2
```

### Related Commands

#### 13.8.14 rpl neighbor

#### Command Purpose

Use this command to set the rpl neighbor of a g8032 ring. Use the no form of this command to delete the rpl neighbor.

#### Command Syntax

```
rpl neighbor (east-interface | west-interface )
no rpl neighbor
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>east-interface</td>
<td>Specify ring's east interface as the RPL neighbor</td>
<td>-</td>
</tr>
<tr>
<td>west-interface</td>
<td>Specify ring's west interface as the RPL neighbor</td>
<td>-</td>
</tr>
</tbody>
</table>

#### Command Mode

**G8032 Configuration**

### Default

None

### Usage

None

### Examples

The following example shows how to set rpl neighbor of a g8032 ring:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# g8032 ring-id 1 east-interface eth-0-1 west-interface eth-0-2
Switch(g8032-ring-1)# rpl neighbor east-interface
Switch(g8032-ring-1)#
```
The following example shows how to delete rpl neighbor of a g8032 ring:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# g8032 ring-id 1 east-interface eth-0-1 west-interface eth-0-2
Switch(g8032-ring-1)# rpl neighbor east-interface
Switch(g8032-ring-1)# no rpl neighbor
```

**Related Commands**
show g8032

**13.8.15 virtual-channel enable**

**Command Purpose**
Use this command to enable sub-ring virtual channel in the g8032 sub ring.

**Command Syntax**
virtual-channel enable

**Command Mode**
G8032 Configuration

**Default**
None

**Usage**
Use this command to enable sub-ring virtual channel. Therefore g8032 sub ring R-APS packets won't be ended in interconnection node.

**Examples**

The following example shows how to enable virtual channel:
```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# g8032 ring-id 1 east-interface eth-0-1 west-interface eth-0-2
Switch(config)# g8032-ring-1# exit
Switch(config)# g8032 ring-id 2 interface eth-0-3 major-ring-id 1
Switch(config)# g8032-ring-2# virtual-channel enable
```

**Related Commands**
show g8032

**13.8.16 mode**

**Command Purpose**
Use this command to set the revertive mode of g8032 ring protection.
Use the no form of this command to return to the default setting.

**Command Syntax**
mode ( revertive | non-revertive )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>revertive</td>
<td>Revertive mode</td>
<td>-</td>
</tr>
<tr>
<td>non-revertive</td>
<td>Non-revertive mode</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**
G8032 Configuration
Default
Revertive mode

Usage
None

Examples
The following example shows how to change the revertive mode of a g8032 ring:
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# g8032 ring-id 1 east-interface eth-0-1 west-interface eth-0-2
Switch(g8032-ring-1)# mode non-revertive

Related Commands
show g8032

13.9  UDLD Commands

13.9.1  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

13.9.2  udld port

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

Command Syntax
udld port (aggressive | )
no udld port
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggressive</td>
<td>UDLD aggressive mode</td>
<td>-</td>
</tr>
</tbody>
</table>

**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

**13.9.3 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>UDLD message interval (seconds). The range is 1-90</td>
<td>1-90 seconds</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

15s

**Usage**

None

**Examples**

This example shows how to set UDLD message interval to 5 seconds:

Switch# configure terminal
Switch(config)# udld message interval 5

**Related Commands**

show udld
13.9.4  udld reset

Command Purpose
Use this command to reset the interfaces disabled by UDLD.

Command Syntax
udld reset

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to reset interfaces disabled by UDLD:
Switch# udld reset

Related Commands
None

13.9.5  show udld

Command Purpose
Use this command to show UDLD information of interfaces.

Command Syntax
show udld ( IFNAME | )

Parameter | Parameter Description | Parameter Value
--- | --- | ---
IFNAME | Interface name | Support physical ports

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to show UDLD information of interface eth-0-1:
Switch# show udld eth-0-1

Interface eth-0-1
...
UDLD mode : aggressive mode
Operational state : Bidirectional
Message interval : 15
Time out interval : 3
Neighbor 1

---
Device ID : 001e.0808.0360
Port ID : eth-0-2
Device Name : DUT2
Message Interval : 15
Timeout Interval : 3
Link status : Bidirectional
Expiration time : 40

Related Commands
None

13.9.6 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

<table>
<thead>
<tr>
<th>Port</th>
<th>Device Name</th>
<th>Device ID</th>
<th>Port ID</th>
<th>Neighbor State</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-0-9</td>
<td>DUT2</td>
<td>d4f2.489f.d100</td>
<td>eth-0-9</td>
<td>bidirectional</td>
</tr>
</tbody>
</table>

Related Commands
None
13.9.7 debug udld

**Command Purpose**
Use this command to debug UDLD.

**Command Syntax**
d debug udld ( all | packet | events )
n debug udld ( all | packet | events )

---

### Table: Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Show both packet and events</td>
<td>-</td>
</tr>
<tr>
<td>packet</td>
<td>Show packets only</td>
<td>-</td>
</tr>
<tr>
<td>events</td>
<td>Show events only</td>
<td>-</td>
</tr>
</tbody>
</table>

**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

13.9.8 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
13.10 ERPS Commands

13.10.1 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAINID</td>
<td>ERPS domain ID.</td>
<td>1-255</td>
</tr>
<tr>
<td>ERPS_NAME</td>
<td>ERPS domain name</td>
<td>String with up to 15 characters</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage

This command is used to create or delete an erps domain. The command should be used first when 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

13.10.2 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAINID</td>
<td>ERPS domain ID.</td>
<td>1-255</td>
</tr>
<tr>
<td>primary</td>
<td>primary ring</td>
<td>-</td>
</tr>
<tr>
<td>sub</td>
<td>sub ring</td>
<td>-</td>
</tr>
<tr>
<td>VLANID</td>
<td>vlan id</td>
<td>2-4094</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration
Default
None

Usage
The erps protocol packet is transferred in the control vlan. It is best to add the control vlan into the instance which is bound by the domain.

Examples
This example shows how to set vlan 15 as primary control vlan for erps domain 11:
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 15
Switch(config-vlan)# exit
Switch(config)# erps 11 primary control vlan 15

Related Commands
show erps

13.10.3 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAINID</td>
<td>ERPS domain ID.</td>
<td>1-255</td>
</tr>
<tr>
<td>HELLOTIME</td>
<td>Hello timer interval</td>
<td>1-150 in the multiple of 100 ms</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
The default hellotime is 10 (1 second), unit is 100ms

Usage
The timer should be the same of all nodes in the ring.

Examples
This example shows how to set hello timer interval of erps domain 11 to 20s:
Switch# configure terminal
Switch(config)# erps 11 hellotime 20

Related Commands
show erps
13.10.4 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAINID</td>
<td>ERPS domain ID.</td>
<td>1-255</td>
</tr>
<tr>
<td>FAILTIME</td>
<td>Fail timer interval</td>
<td>3-450 in the multiple of 100 ms</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

The default failtime is 30(3 second), unit is 100ms

Usage

The timer should be the same of all nodes in the ring.

Examples

This example shows how to set fail timer interval of erps domain 11 to 60s:

```
Switch# configure terminal
Switch(config)# erps 11 failtime 60
```

Related Commands

show erps

13.10.5 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 instance
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAINID</td>
<td>ERPS domain ID</td>
<td>1-255</td>
</tr>
<tr>
<td>INSTANCE_ID</td>
<td>MSTP instance.</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration
**Default**

None

**Usage**

No default instance is specified.

**Examples**

This example shows how to set instance 1 as ERPS11’s protected instance:

Switch#configure terminal

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

Switch(config)# erps 11 mstp instance 1

**Related Commands**

show erps

**13.10.6  erps ring level**

**Command Purpose**

Use this command to create an ERPS ring for specific ERPS domain. Use the no form of this command to remove the ERPS ring.

**Command Syntax**

```
erps DOMAINID ring RINGID level (primary | sub )
no erps DOMAINID ring RINGID
```

**Parameter** | **Parameter Description** | **Parameter Value**
--- | --- | ---
DOMAINID | ERPS domain ID | 1-255
RINGID | ERPS ring ID | 1-255
primary | Primary ring | -
sub | Sub ring | -

**Command Mode**

Global Configuration

**Default**

None

**Usage**

The rings in the erps domain are divided into primary and subrings that are differentiated by the configuration.

**Examples**

This example shows how to create a sub ring with ID 1 for ERPS domain 11:

Switch# configure terminal

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

Switch(config)# erps 11 ring 1 level sub

**Related Commands**

show erps
13.10.7 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**

```plaintext
erps DOMAINID ring RINGID mode ( master | transit | vpls )
no erps DOMAINID ring RINGID mode
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAINID</td>
<td>ERPS domain ID</td>
<td>1-255</td>
</tr>
<tr>
<td>RINGID</td>
<td>ERPS ring ID</td>
<td>1-255</td>
</tr>
<tr>
<td>master</td>
<td>Master node</td>
<td>-</td>
</tr>
<tr>
<td>transit</td>
<td>Transit node</td>
<td>-</td>
</tr>
<tr>
<td>vpls</td>
<td>VPLS node</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

The mode is not set by default.

**Usage**

The master node is used to send and receive erps protocol packet. The transit and vpls node is used to transfer erps protocol packet to neighbor switch.

**Examples**

This example shows how to set node as ERPS domain 11 ring 1 transit node:

```
Switch# configure terminal
Switch(config)# erps 11 ring 1 mode transit
```

**Related Commands**

show erps

13.10.8 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**

```plaintext
erps DOMAINID ring RINGID primary interface ( IFPHYSICAL | IFAGG )
no erps DOMAINID ring RINGID primary interface
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAINID</td>
<td>ERPS domain ID</td>
<td>1-255</td>
</tr>
<tr>
<td>RINGID</td>
<td>ERPS ring ID</td>
<td>1-255</td>
</tr>
<tr>
<td>IFPHYSICAL</td>
<td>Ethernet interface name</td>
<td>-</td>
</tr>
<tr>
<td>IFAGG</td>
<td>Link aggregation interface name</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

None

**Usage**

For master node, the interface with type primary is used to send erps protocol packet. Only the interface in trunk/dot1q-tunnel mode can be set as primary interface.

**Examples**

This example shows how to set interface eth-0-9 as primary interface for ERPS domain 11 ring 1:

```
Switch# configure terminal
Switch(config)# interface eth-0-9
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 15
Switch(config-if)# exit
Switch(config)# erps 11 ring 1 primary interface eth-0-9
```

**Related Commands**

show erps

### 13.10.9 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAINID</td>
<td>ERPS domain ID</td>
<td>1-255</td>
</tr>
<tr>
<td>RINGID</td>
<td>ERPS ring ID</td>
<td>1-255</td>
</tr>
<tr>
<td>IFPHYSICAL</td>
<td>Ethernet interface name</td>
<td>-</td>
</tr>
<tr>
<td>IFAGG</td>
<td>Link aggregation interface name</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration
Default

None

Usage

Only the interface in trunk/dot1q-tunnel mode can be set as secondary interface.

Examples

This example shows how to set interface eth-0-9 as primary interface for ERPS domain 11 ring 1:

```
Switch# configure terminal
Switch(config)#interface eth-0-9
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add 15
Switch(config-if)#exit
Switch(config)#erps 11 ring 1 secondary interface eth-0-9
```

Related Commands

show erps

13.10.10 erps ring interface

Command Purpose

Use this command to set vpls interface for specific ERPS ring instance.
Use no form of this command to unset vpls interface for specific ERPS ring instance.

Command Syntax

```
erps DOMAINID ring DOMAINID interface (IFPHYSICAL | IFAGG)
no erps DOMAINID ring DOMAINID interface
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAINID</td>
<td>ERPS domain ID</td>
<td>1-255</td>
</tr>
<tr>
<td>RINGID</td>
<td>ERPS ring ID</td>
<td>1-255</td>
</tr>
<tr>
<td>IFPHYSICAL</td>
<td>Ethernet interface name</td>
<td>-</td>
</tr>
<tr>
<td>IFAGG</td>
<td>Link aggregation interface name</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This example shows how to set interface eth-0-9 as vpls interface for ERPS domain 11 ring 1:

```
Switch# configure terminal
Switch(config)#interface eth-0-9
Switch(config-if)#switchport mode trunk
```
Switch(config-if)#switchport trunk allowed vlan add 15
Switch(config-if)#exit
Switch(config)#erps 11 ring 1 interface eth-0-9

Related Commands

show erps

13.10.11 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 edge-mode

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAINID</td>
<td>ERPS domain ID</td>
<td>1-255</td>
</tr>
<tr>
<td>RINGID</td>
<td>ERPS ring ID</td>
<td>1-255</td>
</tr>
<tr>
<td>edge</td>
<td>Edge node</td>
<td>-</td>
</tr>
<tr>
<td>assistant-edge</td>
<td>Assistant-edge node</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

Both the edge node and the assistant-edge node are special transit nodes.
Once a node is set to edge/assistant-edge node, it will be set to transit node automatically.

Examples

This example shows how to set node as ERPS domain 11 ring 1 edge node:

Switch# configure terminal
Switch(config)# erps 11 ring 1 edge-mode edge

Related Commands

show erps

13.10.12 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
### Command Mode

**Global Configuration**

**Default**

None

**Usage**

Of the two ports via which the edge node (assistant-edge node) accesses the subring, one is a common port and the other is an edge port. The common port is the port for the edge node (assistant-edge node) to access the primary ring and the subring, while the edge port is the port for the edge node to access the subring only. This command is only available for edge/assistant-edge node.

**Examples**

This example shows how to set interface eth-0-9 as edge interface for ERPS domain 11 ring 1:

```
Switch# configure terminal  
Switch(config)# interface eth-0-9  
Switch(config-if)# switchport mode trunk  
Switch(config-if)# switchport trunk allowed vlan add 15  
Switch(config-if)# exit  
Switch(config)# erps 11 ring 1 edge interface eth-0-9
```

**Related Commands**

`show erps`

### 13.10.13 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAINID</td>
<td>ERPS domain ID</td>
<td>1-255</td>
</tr>
<tr>
<td>RINGID</td>
<td>ERPS ring ID</td>
<td>1-255</td>
</tr>
<tr>
<td>IFPHYSICAL</td>
<td>Ethernet interface name</td>
<td>-</td>
</tr>
<tr>
<td>IFAGG</td>
<td>Link aggregation interface name</td>
<td>-</td>
</tr>
</tbody>
</table>
Default
None

Usage
Of the two ports via which the edge node (assistant-edge node) accesses the subring, one is a common port and the other is an edge port. The common port is the port for the edge node (assistant-edge node) to access the primary ring and the subring, while the edge port is the port for the edge node to access the subring only. This command is only available for edge/assistant-edge node.

Examples
This example shows how to set interface eth-0-9 as edge interface for ERPS domain 11 ring 1:

```
Switch# configure terminal
Switch(config)# interface eth-0-9
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 15
Switch(config-if)# exit
Switch(config)# erps 11 ring 1 common interface eth-0-9
```

Related Commands
show erps

13.10.14 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)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAINID</td>
<td>ERPS domain ID</td>
<td>1-255</td>
</tr>
<tr>
<td>RINGID</td>
<td>ERPS ring ID</td>
<td>1-255</td>
</tr>
<tr>
<td>enable</td>
<td>Enable the srpt</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>Disable the srp</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
None

Examples
This example shows how to enable srpt functionality for ERPS domain 11 ring 1:
```
Switch# configure terminal
Switch(config)# erps 11 ring 1 srpt enable
```
Related Commands
show erps

13.10.15 erps ring enable

Command Purpose
Use this command to enable specific erps ring instance.

Command Syntax
erps DOMAINID ring RINGID enable

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAINID</td>
<td>ERPS domain ID</td>
<td>1-255</td>
</tr>
<tr>
<td>RINGID</td>
<td>ERPS ring ID</td>
<td>1-255</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
Upon the specific ERPS ring is enabled successfully, the ring state should leave the idle state.

Examples
This example shows how to enable ERPS domain 11 ring 1:
Switch# configure terminal
Switch(config)#erps 11 ring 1 enable

Related Commands
show erps

13.10.16 erps ring disable

Command Purpose
Use this command to disable specific erps ring instance.

Command Syntax
erps DOMAINID ring RINGID disable

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAINID</td>
<td>ERPS domain ID</td>
<td>1-255</td>
</tr>
<tr>
<td>RINGID</td>
<td>ERPS ring ID</td>
<td>1-255</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration
**Default**

None

**Usage**

Upon the specific ERPS ring is enabled successfully, the ring state should leave the idle state.

**Examples**

This example shows how to disable ERPS domain 11 ring 1:

```
Switch# configure terminal
Switch(config)# erps 11 ring 1 disable
```

**Related Commands**

show erps

**13.10.17  erps enable**

**Command Purpose**

Use this command to enable specific ERPS domain instance.

**Command Syntax**

```
erps DOMAINID enable
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAINID</td>
<td>ERPS domain ID</td>
<td>1-255</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

None

**Usage**

Use this command to enable all the ring of the erps domain. Enable the domain will make all the rings within the domain be enabled. Upon the specific ERPS ring is enabled successfully, the ring state should leave the idle state.

**Examples**

This example shows how to enable erps domain 11:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# erps 11 enable
```

**Related Commands**

show erps

**13.10.18  erps disable**

**Command Purpose**

Use this command to disable specific erps domain instance.
Command Syntax

```
erps DOMAINID disable
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAINID</td>
<td>ERPS domain ID</td>
<td>1-255</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

Use this command to disable all the ring of the erps domain. Enable the domain will make all the rings within the domain be enabled. Upon the specific ERPS ring is enabled successfully, the ring state should leave the idle state.

Examples

This example shows how to disable erps domain 11:

```
Switch# configure terminal
Switch(config)# erps 11 disable
```

Related Commands

show erps

13.10.19  erps mode rrpp

Command Purpose

Use this command to compatible with RRPP.

Command Syntax

```
erps mode rrpp
no erps mode rrpp
```

Command Mode

Global Configuration

Default

None

Usage

This command to compatible with RRPP.

Examples

This example shows how to compatible with RRPP:

```
Switch# configure terminal
Switch(config)# erps mode rrpp
```

Related Commands

None
13.10.20  show erps

Command Purpose
Use this command to show the configuration for specific erps domain.

Command Syntax
show erps DOMAINID

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAINID</td>
<td>ERPS domain ID</td>
<td>1-255</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to display the configuration for erps domain 1:
Switch# show erps 1
ERPS domain ID: 1
ERPS domain name: ERPS001
ERPS domain mode: normal
ERPS domain primary control VLAN ID: 0
ERPS domain sub control VLAN ID: 0
ERPS domain hello timer interval: 1 second(s)
ERPS domain fail timer interval: 3 second(s)

Related Commands
None

13.10.21  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

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>ERPS0011</td>
</tr>
</tbody>
</table>

Related Commands

None

13.10.22 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 ))

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>All domain</td>
<td>-</td>
</tr>
<tr>
<td>domain DOMAINID</td>
<td>ERPS domain ID</td>
<td>1-255</td>
</tr>
<tr>
<td>ring RINGID</td>
<td>ERPS ring ID</td>
<td>1-255</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to clear all domain statistics:

Switch# clear erps counters all

Related Commands

None

13.10.23 debug erps

Command Purpose

Use this command to open the debug functions of ERPS.

Command Syntax

depug erps ( all | dump | events )

no debug erps ( all | dump | events )
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>all debug information</td>
<td>-</td>
</tr>
<tr>
<td>dump</td>
<td>dump debug information</td>
<td>-</td>
</tr>
<tr>
<td>events</td>
<td>events debug information</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

This example shows how to open all debug functions:

```
Switch# debug erps all
```

**Related Commands**

None

### 13.11 Smart-Link Commands

13.11.1 **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, use `no` form of this command.

**Command Syntax**

```
smart-link group GROUP-ID
no smart-link group (GROUP-ID | all)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP-ID</td>
<td>smart-link group ID</td>
<td>1-16</td>
</tr>
<tr>
<td>all</td>
<td>All the smart-link groups have been exist</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

There is no any smart-link group

**Usage**

Up to 16 smart-link groups can be created.
Examples

Create a smart-link group with ID 1:
Switch# configure terminal
Switch(config)# smart-link group 1

Related Commands
show smart-link group

13.11.2 smart-link relay enable

Command Purpose
Use this command to enable the switch to relay the smart-link flush packet. To disable relaying the packets, use no form of this command.

Command Syntax
smart-link relay enable
no smart-link relay enable

Command Mode
Global Configuration

Default
Relaying the smart-link flush packet is enabled.

Usage
By default, the smart-link flush packet could be flooded. Use the command, “no smart-link relay enable”, to disable the packet flooding to other switches.

Examples
The example shows how to enable smart-link relay:
Switch# configure terminal
Switch(config)# smart-link relay enable
The example shows how to disable smart-link relay:
Switch# configure terminal
Switch(config)# no smart-link relay enable

Related Commands
None

13.11.3 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)
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFPHYSICAL</td>
<td>The name of physical interface</td>
<td>-</td>
</tr>
<tr>
<td>IFAGG</td>
<td>The name of link-agg interface, like agg1</td>
<td>-</td>
</tr>
<tr>
<td>master</td>
<td>The interface act as master role</td>
<td>-</td>
</tr>
<tr>
<td>slave</td>
<td>The interface act as slave role</td>
<td>-</td>
</tr>
</tbody>
</table>

**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:
```
### 13.11.4 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 }
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE-ID</td>
<td>MSTP instance ID. The range is 0-4094</td>
<td>0-4094</td>
</tr>
<tr>
<td>all</td>
<td>All the instance have been exist</td>
<td>-</td>
</tr>
</tbody>
</table>

**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 MSTP 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:

1. Switch# configure terminal
2. Switch(config)# smart-link group 1
3. Switch(config-smlk-group)# protected mstp instance 0
4. Switch(config-smlk-group)# protected mstp instance 10
5. Switch(config-smlk-group)# protected mstp instance 100
6. Switch(config-smlk-group)# end
7. Switch# show smart-link group 1

Smart-link group 1 information:
The smart-link group was disabled.

<table>
<thead>
<tr>
<th>state</th>
<th>time</th>
<th>count</th>
<th>Last-time</th>
</tr>
</thead>
</table>

---

S5850 and S8050 Series Switches CLI Reference Guide

www.fs.com
**Related Commands**

show smart-link group

### 13.11.5 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`)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE-ID</td>
<td>MSTP instance ID. The range is 0-4094</td>
<td>0-4094</td>
</tr>
<tr>
<td>all</td>
<td>All the instance have been exist</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Smart-link Configuration

**Default**

There is no load-balancing instance in the smart-link group by default.

**Usage**

Load-balancing instances will be active in the slave interface. If user want to configure load-balancing instances, should before the smart-group is enabled.

**Examples**

This example shows how to set protected instance 10 as the load-balancing instance:

```
Switch# configure terminal
Switch(config)# smart-link group 1
Switch(config-smlk-group)# load-balance instance 10
```

**Related Commands**

show smart-link group
13.11.6 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESTORE-TIME</td>
<td>The restore time of the smart-link group</td>
<td>30-1200 seconds</td>
</tr>
</tbody>
</table>

Command Mode

Smart-link Configuration

Default

The default restore time is 60 seconds.

Usage

When the master interface is resumed, the links will not be immediately restored to the master interface, but will be delayed a while. The delay time is called restore time.

Examples

This example shows how to set restore time as 30 seconds in the smart-link group 1:

```
Switch# configure terminal
Switch(config)# smart-link group 1
Switch(config-smlk-group)# restore time 30
```

Related Commands

show smart-link group

13.11.7 restore enable

Command Purpose

Use this command to enable/disable restoring feature of the smart-link group.

Command Syntax

restore enable
no restore enable

Command Mode

Smart-link Configuration

Default

The restoring feature of the smart-link group is disabled by default.

Usage

When master interface fails, the link will be switched to the slave interface. Then, if master interface is resumed, the link will not be switched back to keep the flow stable by default. If restoring feature is enabled, the link will be switched back.

NOTE: If load-balancing instance is configured, this feature is recommended strongly.
Examples

This example shows how to enable the restoring feature in the smart-link group 1:

Switch# configure terminal
Switch(config)# smart-link group 1
Switch(config-smlk-group)# restore enable

Related Commands

show smart-link group

13.11.8 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN-ID</td>
<td>Flush packet will be sent through this VLAN.</td>
<td>1-4094</td>
</tr>
<tr>
<td>PASSWORD</td>
<td>The simple password of the flush packet</td>
<td>String with up to 15 characters</td>
</tr>
</tbody>
</table>

Command Mode

Smart-link Configuration

Default

There is no flush sender in the smart-link group by default.

Usage

Mac address-table should be updated when a master (forwarding) link goes down and the slave link begins forwarding traffic. Flush packet is used for this purpose.

NOTE: If the control-vlan is not existed in the switch, sending flush packet will fail.

Examples

This example shows how to configure flush sender of the smart-link group 1, control-vlan is 4 and password is "test":

Switch# configure terminal
Switch(config)# smart-link group 1
Switch(config-smlk-group)# flush send control-vlan 4 password simple test

Related Commands

show smart-link group
smart-link flush receive

13.11.9 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:

<table>
<thead>
<tr>
<th>Switch# configure terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# smart-link group 1</td>
</tr>
<tr>
<td>Switch(config-smlk-group)# group enable</td>
</tr>
</tbody>
</table>

Related Commands

show smart-link group

13.11.10 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Flush packet will be sent through this VLAN.</td>
<td>1-4094</td>
</tr>
<tr>
<td>PASSWORD</td>
<td>The simple password of the flush packet</td>
<td>String with up to 15 characters</td>
</tr>
</tbody>
</table>

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":

<table>
<thead>
<tr>
<th>Switch# configure terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# interface eth-0-9</td>
</tr>
<tr>
<td>Switch(config-if)# smart-link flush receive control-vlan 4 password simple test</td>
</tr>
<tr>
<td>Switch(config-if)# end</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Group-ID</th>
<th>State</th>
<th>MASTER</th>
<th>SLAVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>disabled</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Related Commands**
flush
show smart-link

**13.11.11 smart-link tcn enable**

**Command Purpose**
Use this command to enable smart link tcn. To disable the smart-link tcn, used no form of this command.

**Command Syntax**
smart-link tcn enable
no smart-link tcn enable

**Command Mode**
Global Configuration

**Default**
Disable

**Usage**
None

**Examples**
Switch# configure terminal
Switch(config)# no smart-link tcn enable
Switch# configure terminal
Switch(config)# smart-link tcn enable

**Related Commands**
show smart-link

**13.11.12 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>QUERY-COUNT</td>
<td>TCN query count.</td>
<td>1-10</td>
</tr>
</tbody>
</table>
**Command Mode**
Global Configuration

**Default**
2

**Usage**
None

**Examples**
This example shows how to set smart link tcn query count to 5:

```
Switch# configure terminal
Switch(config)# smart-link tcn query-count 5
```

**Related Commands**
show smart-link

**13.11.13  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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>QUERY-INTERVAL</td>
<td>TCN query interval.</td>
<td>1-255 seconds</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
10s

**Usage**
None

**Examples**
This example shows how to set smart link tcn query interval to 50:

```
Switch# configure terminal
Switch(config)# smart-link tcn query-interval 50
```

Switch# configure terminal
Switch(config)# no smart-link tcn query-interval

**Related Commands**
show smart-link
13.11.14 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.

<table>
<thead>
<tr>
<th>Group-ID</th>
<th>State</th>
<th>MASTER</th>
<th>SLAVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enabled</td>
<td>eth-0-1</td>
<td>eth-0-2</td>
</tr>
</tbody>
</table>

Related Commands
None

13.11.15 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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP-ID</td>
<td>Smart-link group ID</td>
<td>1-16</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
This command is used to display detail information of a specified Smart-link group or all Smart-link groups' status.
Examples

Switch# show smart-link group 1

Related Commands

None

13.11.16 clear smart-link statistic

Command Purpose

Use this command to clear the statistic of the smart-link groups.

Command Syntax

clear smart-link statistic

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to clear the statistic of the smart-link groups.

Examples

Switch# clear smart-link statistic

Related Commands

None

13.11.17 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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>All debugging</td>
<td>-</td>
</tr>
<tr>
<td>flush</td>
<td>Smart-Link Flush Packet</td>
<td>-</td>
</tr>
<tr>
<td>instance</td>
<td>Smart-Link Instance</td>
<td>-</td>
</tr>
<tr>
<td>interface</td>
<td>Smart-Link Interface</td>
<td>-</td>
</tr>
<tr>
<td>restore</td>
<td>Smart-Link auto-restore</td>
<td>-</td>
</tr>
<tr>
<td>mib</td>
<td>SNMP MIBs of Smart-Link</td>
<td>-</td>
</tr>
<tr>
<td>trap</td>
<td>SNMP trap of Smart-Link</td>
<td>-</td>
</tr>
</tbody>
</table>
13.12 Multi-Link Commands

13.12.1 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, use no form of this command.

Command Syntax

```
multi-link group GROUP-ID
no multi-link group (GROUP-ID | all)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP-ID</td>
<td>multi-link group ID</td>
<td>1-16</td>
</tr>
<tr>
<td>all</td>
<td>All the multi-link groups have been exist</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
There is no any multi-link group

Usage
Up to 16 multi-link groups can be created.

Examples
Create a multi-link group with ID 1:
Switch# configure terminal
Switch(config)# multi-link group 1

Related Commands
show multi-link group
13.12.2 multi-link relay enable

**Command Purpose**

Use this command to enable the switch to relay the multi-link flush packet. To disable relaying the packets, use no form of this command.

**Command Syntax**

```
multi-link relay enable
no multi-link relay enable
```

**Command Mode**

Global Configuration

**Default**

Relaying the multi-link flush packet is enabled.

**Usage**

By default, the multi-link flush packet could be flooded. Use the command, "no multi-link relay enable", to disable the packet flooding to other switches.

**Examples**

The example shows how to enable multi-link relay:
```
Switch# configure terminal
Switch(config)# multi-link relay enable
```

The example shows how to disable multi-link relay:
```
Switch# configure terminal
Switch(config)# no multi-link relay enable
```

**Related Commands**

None

13.12.3 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)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFPHYSICAL</td>
<td>The name of physical interface, like eth-0-1</td>
<td>-</td>
</tr>
<tr>
<td>IFAGG</td>
<td>The name of link-aggr interface, like agg1</td>
<td>-</td>
</tr>
<tr>
<td>&lt;1-4&gt;</td>
<td>The priority of the interface</td>
<td>1-4</td>
</tr>
<tr>
<td>all</td>
<td>Both of the master and slave interface</td>
<td>-</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>state</th>
<th>time</th>
<th>count</th>
<th>Last-time</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>60</td>
<td>0</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Protected instance:
Load balance instance:

INTERFACE:

<table>
<thead>
<tr>
<th>Role</th>
<th>Member</th>
<th>DownCount</th>
<th>Last-Down-Time</th>
<th>FlushCount</th>
<th>Last-Flush-Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>MASTER</td>
<td>eth-0-9</td>
<td>0</td>
<td>N/A</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td>SLAVE</td>
<td>eth-0-13</td>
<td>0</td>
<td>N/A</td>
<td>0</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Related Commands

show multi-link group
13.12.4 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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE-ID</td>
<td>MSTP instance ID. The range is 0-4094</td>
<td>0-4094</td>
</tr>
<tr>
<td>all</td>
<td>All the instance have been exist</td>
<td>-</td>
</tr>
</tbody>
</table>

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 MSTP 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:

<table>
<thead>
<tr>
<th>Role</th>
<th>Member</th>
<th>DownCount</th>
<th>Last-Down-Time</th>
<th>FlushCount</th>
<th>Last-Flush-Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRI1</td>
<td>eth-0-9</td>
<td>0</td>
<td>N/A</td>
<td>0</td>
<td>N/A</td>
</tr>
</tbody>
</table>
## Related Commands

show multi-link group

### 13.12.5 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 )
```

#### Related Commands

show multi-link group

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE-ID</td>
<td>MSTP instance ID. The range is 0-4094</td>
<td>0-4094</td>
</tr>
<tr>
<td>&lt;2-4&gt;</td>
<td>Set load-balancing port with same priority</td>
<td>-</td>
</tr>
<tr>
<td>all</td>
<td>All the instance have been exist</td>
<td>-</td>
</tr>
</tbody>
</table>

#### Command Mode

Multi-link Group Configuration

#### Default

There is no load-balancing instance in the multi-link group by default.

#### Usage

Load-balancing instances will be active in the slave interface. If user want to configure load-balancing instances, should before the smart-group is enabled.

#### Examples

This example shows how to set protected instance 10 as the load-balancing instance:

```
Switch# configure terminal
Switch(config)# multi-link group 1
Switch(config-multilink-group)# load-balance instance 10 priority 2
```
13.12.6 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESTORE-TIME</td>
<td>The restore time of the multi-link group</td>
<td>30-1200 seconds</td>
</tr>
</tbody>
</table>

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-multipk-group)# restore time 30

Related Commands
show multi-link group

13.12.7 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

13.12.8 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN-ID</td>
<td>Flush packet will be sent through this VLAN.</td>
<td>1-4094</td>
</tr>
<tr>
<td>PASSWORD</td>
<td>The simple password of the flush packet</td>
<td>String with up to 15 characters</td>
</tr>
</tbody>
</table>

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

13.12.9 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

13.12.10 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN-ID</td>
<td>Flush packet will be sent through this VLAN.</td>
<td>1-4094</td>
</tr>
<tr>
<td>PASSWORD</td>
<td>The simple password of the flush packet</td>
<td>String with up to 15 characters</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Group-ID</th>
<th>State</th>
<th>Pri-1</th>
<th>Pri-2</th>
<th>Pri-3</th>
<th>Pri-4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enabled</td>
<td>eth-0-9</td>
<td>eth-0-10</td>
<td>N/A</td>
<td>eth-0-12</td>
</tr>
</tbody>
</table>

**Related Commands**
flush send
show multi-link

### 13.12.11 multi-link tcn enable
**Command Purpose**
Use this command to enable multi-link tcn. To disable the multi-link tcn, used no form of this command.

**Command Syntax**
multi-link tcn enable
no multi-link tcn enable

**Command Mode**
Global Configuration

**Default**
Disable

**Usage**
None

**Examples**
Switch# configure terminal
Switch(config)# multi-link tcn enable
Switch# configure terminal
Switch(config)# no multi-link tcn enable

**Related Commands**
show multi-link

### 13.12.12 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>QUERY-COUNT</td>
<td>TCN query count.</td>
<td>1-10</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
2

Usage
None

Examples
This example shows how to set multi-link tcn query count to 5:
Switch# configure terminal
Switch(config)# multi-link tcn query-count 5

Related Commands
show multi-link

13.12.13 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>QUERY-INTERVAL</td>
<td>TCN query interval.</td>
<td>1-255 seconds</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
10s

Usage
None

Examples
This example shows how to set multi-link tcn query interval to 50:
Switch# configure terminal
Switch(config)# multi-link tcn query-interval 50
This example shows how to restore the default multi-link tcn query interval to 50:
Switch# configure terminal
Switch(config)# no multi-link tcn query-interval

**Related Commands**

show multi-link

**13.12.14 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.

<table>
<thead>
<tr>
<th>Group-ID</th>
<th>State</th>
<th>Pri-1</th>
<th>Pri-2</th>
<th>Pri-3</th>
<th>Pri-4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enabled</td>
<td>eth-0-9</td>
<td>eth-0-10</td>
<td>N/A</td>
<td>eth-0-12</td>
</tr>
</tbody>
</table>

**Related Commands**

None

**13.12.15 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 | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP-ID</td>
<td>Multi-link group ID</td>
<td>1-16</td>
</tr>
</tbody>
</table>
Command Mode
Privileged EXEC

Default
None

Usage
This command is used to display detail information of a specified Multi-link group or all Multi-link groups' status.

Examples
Switch# show multi-link group 1

Related Commands
None

13.12.16 clear multi-link statistic

Command Purpose
Use this command to clear the statistic of the multi-link groups.

Command Syntax
clear multi-link statistic

Command Mode
Privileged EXEC

Default
None

Usage
This command is used to clear the statistic of the multi-link groups.

Examples
Switch# clear multi-link statistic

Related Commands
None

13.12.17 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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>All debugging</td>
<td>-</td>
</tr>
<tr>
<td>flush</td>
<td>Multi-link Flush Packet</td>
<td>-</td>
</tr>
<tr>
<td>instance</td>
<td>Multi-link Instance</td>
<td>-</td>
</tr>
<tr>
<td>interface</td>
<td>Multi-link Interface</td>
<td>-</td>
</tr>
<tr>
<td>restore</td>
<td>Multi-link auto-restore</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None
Examples

Switch# debug multi-link all

Related Commands

None

13.12.18 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFPHYSICAL</td>
<td>The name of physical interface, like eth-0-1</td>
<td>-</td>
</tr>
<tr>
<td>IFAGG</td>
<td>The name of link-agg interface, like agg1</td>
<td>-</td>
</tr>
</tbody>
</table>

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
```

13.12.19 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)
```
### 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

### 13.12.20 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-255&gt;</td>
<td>The interval of sending enhance packets</td>
<td>1-255</td>
</tr>
</tbody>
</table>

**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

13.12.21 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-255&gt;</td>
<td>The interval of checking received enhance packets</td>
<td>1-255</td>
</tr>
</tbody>
</table>

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
13.13 Monitor Link Commands

13.13.1 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP-ID</td>
<td>Monitor link group number</td>
<td>1-16</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
No monitor link group is created

Usage
This command is used to create monitor link group. The group range is 1-16.

Examples
In the following example, monitor link group 1 is created:

Switch# configure terminal
Switch(config)# monitor-link group 1

Related Commands
no monitor-link group

13.13.2 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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFPHYSICAL</td>
<td>Ethernet interface name</td>
<td>-</td>
</tr>
<tr>
<td>IFAGG</td>
<td>Link aggregation interface name</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Monitor-link Configuration

Default
No interface is add
Usage

Only Ethernet interface and aggregation interface can be used as monitor link group.

Examples

In the following example, the ethernet interface is set to monitor link group member:

Switch# configure terminal
Switch(config)# monitor-link group 1
Switch(config-mtlk-group)# monitor-link uplink interface eth-0-1

Related Commands

show monitor-link group

13.13.3 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP-ID</td>
<td>Monitor link group number</td>
<td>1-16</td>
</tr>
</tbody>
</table>

Command Mode

Monitor-link Configuration

Default

No smart link group is add

Usage

Only the smart link group which is enabled can be add to monitor link group

Examples

In the following example, the smart link group is set to monitor link group member:

Switch# configure terminal
Switch(config)# monitor-link group 1
Switch(config-mtlk-group)# monitor-link uplink smart-link group 1

Related Commands

show monitor-link group

13.13.4 no monitor-link uplink

Command Purpose

Use this command to delete all the uplink from monitor link group.

Command Syntax

no monitor-link uplink

Command Mode
Monitor-link Configuration

**Default**
None

**Usage**
This command is used to delete all the uplink from monitor link group.

**Examples**
In the following example, all the uplink is deleted from monitor link group:

```
Switch# configure terminal
Switch(config-mtlk-group)# no monitor-link uplink
```

**Related Commands**
show monitor-link group

### 13.13.5 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)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFPHYSICAL</td>
<td>Ethernet interface name</td>
<td>-</td>
</tr>
<tr>
<td>IFAGG</td>
<td>Link aggregation interface name</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**
Monitor-link Configuration

**Default**
No interface is add

**Usage**
Only Ethernet interface and aggregation interface can be add to monitor link group.

**Examples**
In the following example, the Ethernet interface is set to monitor link group member:

```
Switch# configure terminal
Switch(config)# monitor-link group 1
Switch(config-mtlk-group)# monitor-link downlink interface eth-0-1
```

**Related Commands**
show monitor-link group

### 13.13.6 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`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RECOVER_TIME</td>
<td>Monitor link group recover time range (second)</td>
<td>0-60 seconds</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

The default value is 3 seconds

Usage

This command is used to set recover time for monitor link group. If the uplink is change to up, all the downlink will be set to up after recover timer.

Examples

In the following example, monitor link group's recover-time is set to 1s:

Switch# configure terminal
Switch(config)# monitor-link recover-time 1

Related Commands

show monitor-link group

13.13.7 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 | )`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP-ID</td>
<td>Monitor link group number</td>
<td>1-16</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Role</th>
<th>Member</th>
<th>Last-up-time</th>
<th>Last-down-time</th>
<th>upcount</th>
<th>downcount</th>
</tr>
</thead>
<tbody>
<tr>
<td>UpLk</td>
<td>eth-0-2</td>
<td>2011/07/15,01:34:17</td>
<td>2011/07/15,01:34:14</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Related Commands

None

13.13.8 debug monitor-link

Command Purpose

Use this command to debug monitor link.

Command Syntax

deploy monitor-link

Command Mode

Privileged EXEC

Default

None.

Usage

None.

Examples

In the following example, the debug of monitor link is set to on:

Switch# debug monitor-link

Related Commands

None

13.14 VRRP Commands

13.14.1 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>Time interval between successive advertisements sent by the master virtual router. The unit of the interval is in seconds.</td>
<td>1-255 seconds</td>
</tr>
</tbody>
</table>
Default
Default is 1 second.

Usage
The advertisements sent by the master virtual router communicate the state and priority of the current master virtual router. The advertisement-interval command configures the time between successive advertisement packets and the time before other routers declare the master router to be down. Routers or access servers on which timer value are not configured can learn timer values from the master router. The timers configured on the master router always override any other timer settings. All routers in a VRRP group must use the same timer value. If the same timer value is not set, the routers in the VRRP group will not communicate with each other and any misconfigured router will change its state to master.

Examples
The following example shows how to configure the master virtual router to send advertisements every 4 seconds:

```
Switch# configure terminal
Switch(config)# router vrrp 1
Switch(config-router)# advertisement-interval 4
```

Related Commands
advertisement-interval msec

13.14.2 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>Time interval between successive advertisements sent by the master virtual router. The unit of the interval is in 100 milli-seconds.</td>
<td>100-900 milli-seconds.</td>
</tr>
</tbody>
</table>

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
```

www.fs.com
Switch(config)# router vrrp 1
Switch(config-router)# advertisement-interval msec 100

**Related Commands**
advertisement-interval

**13.14.3 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERFACE-ID</td>
<td>Interface name</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**
Router Configuration

**Default**
None

**Usage**
The max VRPP group number should be no more than 3 for one VRRP interface.

**Examples**
The following is a sample output from the interface command:
Switch# configure terminal
Switch(config)# router vrrp 1
Switch(config-router)# interface eth-0-1

**Related Commands**
router vrrp

**13.14.4 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)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>True</td>
<td>Enable learn advertisement interval</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>from master router</td>
<td></td>
</tr>
<tr>
<td>False</td>
<td>Disable learning advertisement interval</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>from master router</td>
<td></td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# router vrrp 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config-router)# leammaster-mode true</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Related Commands

router vrrp

13.14.5 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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>True</td>
<td>Preemption enabled</td>
<td>-</td>
</tr>
<tr>
<td>False</td>
<td>Preemption disabled</td>
<td>-</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# router vrrp 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config-router)# preempt-mode true</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config-router)# priority 200</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Related Commands

preempt delay
13.14.6 preempt delay

**Command Purpose**
To configure the master down interval when preempt takes effect.

**Command Syntax**
preempt delay time

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIME</td>
<td>Preempt delay time</td>
<td>0-3600 seconds</td>
</tr>
</tbody>
</table>

**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

13.14.7 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>level</td>
<td>Priority of the router within the VRRP group. The range is from 1 to 254.</td>
<td>1-254</td>
</tr>
</tbody>
</table>

**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

route vrrp

13.14.8 route vrrp

Command Purpose

To create a Virtual Router Redundancy Protocol (VRRP) group, use the route vrrp command in Global Configuration mode. To remove this VRRP group, use the no form of this command.

Command Syntax

route vrrp GROUP
no route vrrp GROUP

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP</td>
<td>Group number to which the tracking applies</td>
<td>1-255</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

None

Examples

The following is a sample shows how to create a VRRP group:

Switch# configure terminal
Switch(config)# router vrrp 1

Related Commands

None

13.14.9 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
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OBJ_ID</td>
<td>track object id</td>
<td>1-500</td>
</tr>
<tr>
<td>decrement VALUE</td>
<td>Priority decrement value</td>
<td>1-255</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration

**Default**

None

**Usage**

Use track to monitor an up link interface, so that when the monitoring interface is down, backup can change to master router. Only 1 track object is valid for one special VRRP group, and the later configured track object will always overwrite the previous one.

**Examples**

The following is a sample output from the track command:

```
Switch# configure terminal
Switch(config)# track 10 interface eth-0-1 linkstate
Switch(config)# router vrrp 1
Switch(config-router)# track 10
```

**Related Commands**

router vrrp

13.14.10 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

**13.14.11 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-ADDRESS</td>
<td>IP address of the virtual router</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

**Command Mode**

Router Configuration

**Default**

None

**Usage**

For VRRP to elect a designated router, at least one router on the cable must have been configured with the primary address of the virtual router.

VRRP does not support address learning. All addresses must be configured.

All routers in the VRRP group must be configured with the same primary address for the virtual router. If different primary addresses are configured, the routers in the VRRP group will not communicate with each other and any mis-configured routers in the group will change their state to master.

The virtual IP address must be in the same subnet with VRRP interface, and if virtual IP is equal to the interface IP address, it is called IP address owner.

**Examples**

The following example shows how to enable VRRP on eth-0-1. The VRRP group is 1. IP address 10.0.1.20 is the address of the virtual router:

```
Switch# configure terminal
Switch(config)#interface eth-0-1
Switch(config-if)#no switchport
Switch(config-if)#ip address 10.0.1.1/24
Switch(config)#router vrrp 1
Switch(config-router)#interface eth-0-1
Switch(config-router)#virtual-ip 10.0.1.20
Switch(config-router)#enable
```

**Related Commands**

router vrrp

**13.14.12 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 |)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP</td>
<td>(Optional) Virtual router group number of the group for which information is to be displayed.</td>
<td>1-255</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
If no group is specified, all groups are displayed.

Examples
The following is a sample output from the show vrrp command:

Switch# show vrrp

VRID <1>
State : Master
Virtual IP : 10.0.20.254 (Not IP owner)
Interface : eth-0-10
VMAC : 0000.5e00.0101
Advt timer : 1
Preempt mode : TRUE
Conf pri : 200 Run pri : 200
Master router ip : 10.0.20.1
Master priority : 200
Master advt timer : 1
Master down timer : 3
Preempt delay : 100 second(s)
Learn master mode : FALSE

Related Commands
router vrrp

13.14.13  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
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>The nexthop address of bfd session</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PRIORITY</td>
<td>Increase VRRP priority</td>
<td>1-255</td>
</tr>
</tbody>
</table>

**Command Mode**

**VRRP Configuration**

**Default**

By default IP BFD for VRRP is disabled under each VRRP instance.

**Usage**

Use this command to enable IP BFD for VRRP under each instance.

The IP BFD session should be created after VRRP instance is created and virtual-ip, VRRP interface have both been configured. The IP BFD session should be destroyed when state of links change to down or VRRP instance is deleted.

**Examples**

In the following example, IP BFD for VRRP is enabled under the VRRP instance:

```
Switch# configure terminal
Switch(config)# router vrrp 1
Switch(config-router)# bfd 9.9.9.2
```

In the following example, IP BFD helps VRRP change the running priority other than configured priority when link happen to be down:

```
Switch# configure terminal
Switch(config) # router vrrp 1
Switch(config-router) # bfd 9.9.9.2 increase 30
```

**Related Commands**

None

### 13.15 Track Commands

#### 13.15.1 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>The delay time before the status of track turn up.</td>
<td>1-180 seconds</td>
</tr>
</tbody>
</table>

**Command Mode**

**Track Configuration**

**Default**

By default the delay time is 0.
Usage
None

Examples
In the following example, the delay up command is used to configure delay when object state is turned from down to up:
Switch# configure terminal
Switch(config)# track 1 interface eth-0-1 linkstate
Switch(config-track)# delay up 30

Related Commands
delay down

13.15.2 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>The delay time before the status of track turn down.</td>
<td>1-180 seconds</td>
</tr>
</tbody>
</table>

Command Mode
Track Configuration

Default
By default the delay time is 0.

Usage
None

Examples
In the following example, the delay down command is used to configure delay when object state is turned from up to down:
Switch# configure terminal
Switch(config)# track 1 interface eth-0-1 linkstate
Switch(config-track)# delay down 30

Related Commands
delay up

13.15.3 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
null frequency

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>The frequency of IP SLA operation</td>
<td>1-4800 seconds</td>
</tr>
</tbody>
</table>

**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

13.15.4 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**

```plaintext
ip sla monitor ENTRY-NUMBER
no ip sla monitor ENTRY-NUMBER
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENTRY-NUMBER</td>
<td>Identify of ip sla monitor entry</td>
<td>1-255</td>
</tr>
</tbody>
</table>

**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)#
13.15.5 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>STRING</td>
<td>description string for IP SLA</td>
<td>String with up to 255 characters</td>
</tr>
</tbody>
</table>

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

13.15.6 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)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENTRY-NUMBER</td>
<td>Identify of ip sla monitor entry</td>
<td>1-255</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
None

Examples
In the following example, the ip sla monitor schedule command is used to enable an IP SLA monitor entry:

Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# exit
Switch(config)# ip sla monitor schedule 1

Related Commands
show ip sla monitor
13.15.7 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>Time out value</td>
<td>1-4800 seconds</td>
</tr>
</tbody>
</table>

Command Mode

IP SLA Configuration

Default

The default value is 5 seconds.

Usage

The timeout value should follow this rule:
```
frequency > interval * (packets-per-test - 1) + timeout
```

Examples

In the following example, the timeout command is used to set the time range:
```
Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# timeout 10
```

Related Commands

show ip sla monitor

13.15.8 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MILLISECONDS</td>
<td>The upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.()</td>
<td>1 - 4800000 milliseconds</td>
</tr>
</tbody>
</table>

Command Mode

IP SLA Configuration

Default

The default value is 5000 milliseconds.
Usage
The threshold value should follow this rule:
\[ \text{timeout} \geq \text{threshold} \]

Examples
In the following example, the threshold command is used to set the threshold time range:

Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# threshold 10000

Related Commands
show ip sla monitor

13.15.9 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDS</td>
<td>The interval between probe of each ipsla test</td>
<td>1-4800 seconds</td>
</tr>
</tbody>
</table>

Command Mode
IP SLA Configuration

Default
The default value is 6 seconds.

Usage
The interval value should follow this rule:
\[ (\text{frequency} > \text{interval} \times (\text{packets-per-test} - 1) + \text{timeout}) \]

Examples
In the following example, the interval command is used to set the IP SLA interval:

Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# interval 10

Related Commands
show ip sla monitor

13.15.10 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ttl value</td>
<td>TTL value</td>
<td>1-255</td>
</tr>
<tr>
<td>no ttl</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Command Mode**

IP SLA Configuration

**Default**

64

**Usage**

None

**Examples**

The following example shows how to set TTL for IP SLA:

Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# ttl 100

**Related Commands**

show ip sla monitor

13.15.11 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>tos value</td>
<td>tos value</td>
<td>1-255</td>
</tr>
<tr>
<td>no tos</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Command Mode**

IP SLA Configuration

**Default**

0

**Usage**

None

**Examples**

The following example shows how to set tos for IP SLA:

Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# tos 100

**Related Commands**

show ip sla monitor
13.15.12 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIZE</td>
<td>The protocol data size in the payload of an IP SLAs operation's request packet</td>
<td>1 - 8100</td>
</tr>
</tbody>
</table>

**Command Mode**

IP SLA Configuration

**Default**

28

**Usage**

None

**Examples**

Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# data-size 100

**Related Commands**

show ip sla monitor

13.15.13 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HEX_STRING</td>
<td>Hex string for data pattern</td>
<td>0-0xFFFFFFFF</td>
</tr>
</tbody>
</table>

**Command Mode**

IP SLA Configuration

**Default**

ABCDABCD

**Usage**

None
Examples

Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# data-pattern abababab

Related Commands

show ip sla monitor

13.15.14 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERCENT</td>
<td>The fail percent used to judge test result</td>
<td>1-100</td>
</tr>
</tbody>
</table>

Command Mode

IP SLA Configuration

Default

100

Usage

None

Examples

Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# fail-percent 100

Related Commands

show ip sla monitor

13.15.15 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>The probe count of each test</td>
<td>1-10</td>
</tr>
</tbody>
</table>
**Command Mode**

IP SLA Configuration

**Default**

3

**Usage**

The packets-per-test value should follow this rule:

\[ \text{frequency} > \text{interval} \times (\text{packets-per-test} - 1) + \text{timeout} \]

**Examples**

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

**Related Commands**

show ip sla monitor

---

### 13.15.16  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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKT_CNT</td>
<td>Packet Number for statistic</td>
<td>0-1000</td>
</tr>
<tr>
<td>TEST_CNT</td>
<td>The count of test for statistic</td>
<td>1-10</td>
</tr>
</tbody>
</table>

**Command Mode**

IP SLA Configuration

**Default**

packet: 50; test: 5

**Usage**

None

**Examples**

Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# statistics packet 60
Switch(config-ipsla)# statistics test 6

**Related Commands**

show ip sla monitor
### 13.15.17  clear ip sla statistics

**Command Purpose**
Use this command to clear ipsla statistics.

**Command Syntax**
clear ip sla statistics ENTRY_ID

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENTRY_ID</td>
<td>IP SLA entry id</td>
<td>1-255</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
Switch# clear ip sla statistics 1

**Related Commands**
show ip sla monitor

### 13.15.18  track

**Command Purpose**
To configure a track object, use the track command in Global Configuration mode.

**Command Syntax**
track OBJECT_ID

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OBJECT_ID</td>
<td>Object identity is used to identify track object</td>
<td>1-500</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
None

**Usage**
None

**Examples**
In the following example, the track command is used to create a track object:
Switch# configure terminal
Switch(config)# track 1 interface eth-0-1 linkstate
Switch(config-track)#

**Related Commands**
show track
13.15.19  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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OBJECT_ID</td>
<td>Object identity is used to identify track object</td>
<td>1-500</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical/aggregation/loopback/vlan/tunnel ports</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
None

Examples
In the following example, the track interface linkstate command is used to create an track object:

Switch# configure terminal
Switch(config)# track 1 interface eth-0-1 linkstate
Switch(config-track)#

Related Commands
show track

13.15.20  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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OBJECT_ID</td>
<td>Object identity is used to identify track object</td>
<td>1-500</td>
</tr>
<tr>
<td>ENTRY_ID</td>
<td>IP SLA entry id</td>
<td>1-255</td>
</tr>
</tbody>
</table>
**Command Mode**
Global Configuration

**Default**
None

**Usage**
None

**Examples**
In the following example, the track rtr reachability command is used to create a track object:

```
Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# exit
Switch(config)# track 1 rtr 1 reachability
Switch(config-track)#
```

**Related Commands**
show track

**13.15.21 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OBJECT_ID</td>
<td>Object identity is used to identify track object</td>
<td>1-500</td>
</tr>
<tr>
<td>ENTRY_ID</td>
<td>IP SLA entry id</td>
<td>1-255</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
None

**Usage**
None

**Examples**
In the following example, the track rtr state command is used to create a track object:

```
Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# exit
Switch(config)# track 1 rtr 1 state
```
Switch(config-track)#

Related Commands

show track

13.15.22 track bfd

Command Purpose

Create a track object and track the state of bfd session, use the track bfd command in Global Configuration mode. To remove a track, use the no form of this command. When the state of bfd session is up, track object state is up; otherwise track object state is down.

Command Syntax

track OBJECT_ID bfd source interface IFNAME destination IP_ADDR
no track OBJECT_ID

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OBJECT_ID</td>
<td>Object identity is used to identify track object</td>
<td>1-500</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical/aggregation/vlan/ports</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>Destination IP address of the bfd session</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default
None

Usage
The source interface should be a Layer 3 interface and ip address should be configured. The destination ip address should be in the same network of the interface ip address.

Examples

In the following example, the track bfd command is used to create a track object:

Switch# configure terminal
Switch(config)# interface eth-0-9
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 9.9.9.1/24
Switch(config-if)# quit
Switch(config)# track 1 bfd source interface eth-0-9 destination 9.9.9.2
Switch(config-track)#

Related Commands

show track
13.15.23  track bfd session

Command Purpose
Create a track object and track the state of bfd session, use the track bfd session command in Global Configuration mode. To remove a track, use the no form of this command.
When the state of bfd session is up, track object state is up; otherwise track object state is down.

Command Syntax
track OBJECT_ID bfd session SESSION_NAME
no track OBJECT_ID

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OBJECT_ID</td>
<td>Object identity is used to identify track object</td>
<td>1-500</td>
</tr>
<tr>
<td>SESSION_NAME</td>
<td>BFD session name</td>
<td>String up to 16 characters</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
The bfd session should be created before this command configure.

Examples
In the following example, the track bfd session command is used to create a track object:
Switch# configure terminal
Switch(config)# bfd test peer-ip 9.9.9.2 source 10.10.10.1 local 10 remote 20
Switch(config)# track 1 bfd session test
Switch(config-track)#

Related Commands
show track

13.15.24  type icmp-echo

Command Purpose
Use this command to define 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>Destination IP address of sending icmp packet</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>source-interface IFNAME</td>
<td>Source interface of sending icmp packet</td>
<td>Support physical/aggregation/vlan/ports</td>
</tr>
<tr>
<td>SRC_IP_ADDR</td>
<td>Source IP address of sending icmp packet</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>
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

13.15.25 show ip sla monitor

Command Purpose
To show IP SLA entries, packet statistics and recent test result, use show ip sla monitor in EXEC mode.

Command Syntax
show ip sla monitor (ENTRY_ID) (statistics (packet | test) | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENTRY_ID</td>
<td>Entry number is used to identify ip sla monitor entry, its range is from 1 to 255</td>
<td>1-255</td>
</tr>
</tbody>
</table>

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
### show track

**Command Purpose**
To show TRACK entries, use show track in EXEC mode.

**Command Syntax**

```plaintext
show track OBJECT_ID
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OBJECT_ID</td>
<td>Object identity is used to identify track object</td>
<td>1-500</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Type</th>
<th>Response Time Reporter(RTR) Reachability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>eth-0-2</td>
</tr>
<tr>
<td>State</td>
<td>down</td>
</tr>
<tr>
<td>Delay up</td>
<td>30 seconds</td>
</tr>
<tr>
<td>Delay down</td>
<td>30 seconds</td>
</tr>
</tbody>
</table>

**Related Commands**

Track

### 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>VRF name</td>
<td>String with up to 15 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

IP SLA Configuration

**Default**

None

**Usage**

None

**Examples**

In the following example, the vrf command is used to use ip sla monitor entry in VPN:

```
Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# vrf vpn1
```

**Related Commands**

show ip sla monitor

---

**13.16 VARP Commands**

**13.16.1 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-addr</td>
<td>Virtual mac address</td>
<td>MAC Address</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

None

**Usage**

This virtual mac is used for interface configured virtual IP address. The address is receive-only; the switch never sends packets with this address as the source. And it only exists in ARP replay for virtual IP.
Examples

The following example is the result of this command:

Switch# configure terminal
Switch(config)# ip virtual-router mac 1.1.1

Related Commands

ip virtual-router address

13.16.2 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D</td>
<td>Virtual IP address without mask</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>A.B.C.D/M</td>
<td>Virtual IP address with mask</td>
<td>IPv4 Address and mask length</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

None

Usage

The ip virtual-router address command assigns a virtual IP address to the interface. The virtual IP address without mask should be in the subnet of the primary IP address assigned to the interface and the virtual IP address with mask should not be in the subnet of the primary IP address assigned to the interface. The virtual IP address without mask and the virtual IP address with mask must be selected only one to be configured. If virtual mac is not configured, there is no reply to ARP request packet for the virtual IP address.

Examples

The following example is the result of this command:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ip virtual-router address 1.1.1.1

Related Commands

ip virtual-router mac

13.17 IP BFD Commands

13.17.1 bfd interval

Command Purpose

Use this command to specify the desired transmit interval, receive interval and detect multiplier of IP BFD on the interface. Use the "no" form of this command to restore the default value.
**Command Syntax**
```
bfd interval { tx MINTX | rx MINRX | multiplier MULTIPLIER }
no bfd interval
```

**Command Mode**
Interface Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MINTX</td>
<td>Set BFD minimum transmit interval</td>
<td>3-1000 millisecond</td>
</tr>
<tr>
<td>MINRX</td>
<td>Set BFD minimum receive interval</td>
<td>3-1000 millisecond</td>
</tr>
<tr>
<td>MULTIPLIER</td>
<td>Set the value of Hello Multiplier</td>
<td>2-15</td>
</tr>
</tbody>
</table>

**Default**
The default value for minimum tx interval and rx interval is 20ms.
The default value for detect multiple is 3.

**Usage**
Use this command to specify the transmit interval, receive interval and detect multiple of IP BFD on the interface.
This configuration should affect all the IP BFD sessions on this interface. The actual transmit interval and receive interval need to negotiate with another end of the session.

**Examples**
In the following example, the desired transmit interval is set as 3 ms, the desired receive interval is set as 3 ms, the detect multiplier is set as 3 times:
```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# bfd interval mintx 3 minrx 3 multiplier 3
```

**Related Commands**
None

13.17.2 **bfd NAME peer-ip A.B.C.D interface**

**Command Purpose**
Use this command to configure one Single-hop IP BFD session.
Use the “no” form of this command to remove the session

**Command Syntax**
```
bfd NAME peer-ip A.B.C.D ( vrf NAME | ) interface ( IFPHYSICAL | IFVLAN | IFAGG ) ( source-ip A.B.C.D | ) ( auto | local LDISR remote RDISR )
no bfd NAME
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer-ip A.B.C.D</td>
<td>BFD destination ip address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>vrf NAME</td>
<td>specify a vrf for bfd</td>
<td>-</td>
</tr>
<tr>
<td>interface</td>
<td>specify an interface for single hop</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>bfd</td>
<td></td>
</tr>
<tr>
<td>Source-ip A.B.C.D</td>
<td>specify source ip address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>auto</td>
<td>Allocating local discriminator by system</td>
<td></td>
</tr>
<tr>
<td>LDISR</td>
<td>specify local discriminator by users</td>
<td>1-8191</td>
</tr>
<tr>
<td>RDISR</td>
<td>specify local discriminator by users</td>
<td>1-8191</td>
</tr>
</tbody>
</table>
Command Mode
Global Configuration

Default
By default there is no IP Single BFD session to be created.

Usage
Use this command to specify the IP BFD for static route. BFD session is created, the bfd configurations need meet the following conditions:
- The destination ip address should be subnet with the ip address of the binded interface.
- The specified vrf should be same as that of the binded interface. If users don't specify the vrf, the bfd vrf would be default.
- The source ip address should be same as that of the binded interface. If users don't specify the source ip address, the source ip would be got from the binded interface, which is subnet with the destination ip address. If there are many ip addresses of the binded interface subnet the the destination ip address, the primary ip address would be selected firstly, and the smaller values of the ip addresses would be chosen secondly.

If users specify the local and remote discriminator, bfd uses them. Otherwise, the bfd local discriminator would be allocated by system.

Examples
In the following example, the single-hop IP bfd session “test” is created:
Switch(config)# configure terminal
Switch(config)# bfd test peer-ip 9.9.9.2 interface eth-0-9 local 10 remote 20

Related Commands
ip route

13.17.3 bfd NAME peer-ip A.B.C.D source-ip

Command Purpose
Use this command to configure one Multi-hop IP BFD session. Use the "no" form of this command to remove this configuration.

Command Syntax
`bfld NAME peer-ip A.B.C.D source-ip A.B.C.D ( auto | local LDISR remote RDISR )`
`no bfd NAME`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>BFD name</td>
<td>String with up to 16 characters</td>
</tr>
<tr>
<td>peer-ip A.B.C.D</td>
<td>BFD destination ip address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>Source-ip A.B.C.D</td>
<td>specify source ip address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>auto</td>
<td>Allocating local discriminator by system</td>
<td>-</td>
</tr>
<tr>
<td>LDISR</td>
<td>specify local discriminator by users</td>
<td>1-8191</td>
</tr>
<tr>
<td>RDISR</td>
<td>specify local discriminator by users</td>
<td>1-8191</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration
By default there is no IP Multiple BFD session to be created.

**Usage**

Use this command to specify the IP BFD for static route. BFD session is created, the bfd configurations need meet the following conditions:

1. The source ip address should be same as that of the local L3 interface.
2. If users specify the local and remote discriminator, bfd uses them. Otherwise, the bfd local discriminator would be allocated by system.

**Examples**

In the following example, the multi-hop IP bfd session "test" is created:

```bash
Switch(config)# bfd test peer-ip 9.9.9.2 source 10.10.10.1 local 10 remote 20
```

**Related Commands**

- `ip route` (13.17.4)

**Command Purpose**

Use this command to specify to bind IP BFD session for static route. Use the "no" form of this command to remove this configuration.

**Command Syntax**

```
ip route PREFIX NEXTHOP bind bfd NAME
no ip route prefix nexthop bind bfd
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PREFIX</td>
<td>IP destination prefix (e.g. 10.0.0.0/8)</td>
<td>IPv4 Address and mask length</td>
</tr>
<tr>
<td>NEXTHOP</td>
<td>IP gateway address</td>
<td>-</td>
</tr>
<tr>
<td>NAME</td>
<td>bfd session name</td>
<td>String with up to 16 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

By default there is no IP BFD session to be binded with one static route.

**Usage**

Use this command to bind an existent IP BFD session for static route. The session should be create before use this command. When the ip static route is deleted, the session should be detach from the route, but not destroyed.

**Examples**

In the following example, the IP bfd session "test" is bound to the static router 1.1.1.0/24 via 9.9.9.2:

```bash
Switch(config)# ip route 1.1.1.0/24 9.9.9.2 bind bfd test
```

**Related Commands**

- `ip route`
### 13.17.5 bfd set interval

**Command Purpose**
Use this command to configure the interval of sending and receiving bfd packets for bfd session. Use the "no" form of this command to remove this configuration.

**Command Syntax**
```
bfd set interval mintx MINTX minrx MINRX multiplier MULTIPLIER
no bfd set interval
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MINTX</td>
<td>The minimum interval of sending bfd packets</td>
<td>3-1000 millisecond</td>
</tr>
<tr>
<td>MINRX</td>
<td>The minimum interval of receiving bfd packets</td>
<td>3-1000 millisecond</td>
</tr>
<tr>
<td>MULTIPLIER</td>
<td>the times of timeout</td>
<td>2-15</td>
</tr>
</tbody>
</table>

**Command Mode**
BFD Configuration

**Default**
By default, the minimum time of sending and receiving packets are respectively 20ms and 20ms, the times of timeout is 3.

**Usage**
Use this command to specify the mintx, minrx and timeout of bfd session.

**Examples**
In the following example, set the interval of sending and receiving bfd packets for bfd session "test":
```
Switch# configure terminal
Switch(config)## bfd test
Switch(config-ip-bfd)bfd set interval mintx 30 minrx 30 multiplier 5
```

**Related Commands**
show bfd session detail

### 13.17.6 bfd global dscp

**Command Purpose**
Use this command to configure global dscp value for all multi-hop bfd sessions. Use the "no" form of this command to remove this configuration.

**Command Syntax**
```
bfd set dscp DSCP
no bfd global dscp
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP</td>
<td>the dscp value of bfd packet in IP head</td>
<td>0-63</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration
Default

By default, the dscp value of all the multi-hop bfd sessions is 56.

Usage

Use this command to specify the dscp for all the multi-hop bfd sessions.

Examples

In the following example, user configures to set the global dscp value for all the multi-hop for all the bfd sessions:

```
Switch# configure terminal
Switch(config)# bfd global dscp 63
```

Related Commands

show bfd session detail

13.17.7 bfd set dscp

Command Purpose

Use this command to configure global dscp value for one multi-hop bfd session.
Use the "no" form of this command to remove this configuration.

Command Syntax

```
bfd set dscp DSCP
no bfd set dscp
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP</td>
<td>the dscp value of bfd packet in IP head</td>
<td>0-63</td>
</tr>
</tbody>
</table>

Command Mode

BFD Configuration

Default

By default, the dscp value of one multi-hop bfd sessions is 56.

Usage

Use this command to specify the dscp for one multi-hop bfd session.
When removing this configuration, the dscp of this multiplier bfd session would be the global dscp value when configuring the global dscp.

Examples

In the following example, user configures to set the global dscp value for all the multi-hop for all the bfd sessions:

```
Switch# configure terminal
Switch(config) bfd test
Switch(config-ip-bfd)# bfd set dscp 63
```

Related Commands

show bfd session detail

13.17.8 show bfd

Command Purpose

Use this command to show the statues of IP BFD module.
**Command Syntax**

show bfd

**Command Mode**

Privileged EXEC

**Default**

N/A

**Usage**

Use this command to show the statues of IP BFD module.

**Examples**

The following example is the result of this command:

```
Switch# show bfd

BFD ID: 00    Start Time:Thu May 2 03:09:41 2013
Number of Sessions: 2
Slow Timer: 1000    Image type: DISTRIBUTED
Echo Mode: Disabled    BFD Notifications disabled
Next Session Discriminator: 10
BFD Clients:
    STATIC -> Client ID: 1
    OSPF -> Client ID: 4

```

**Related Commands**

None

**13.17.9 show bfd static configurations**

**Command Purpose**

Use this command to show the bfd static configurations.

**Command Syntax**

show bfd static configurations ( word )

**Command Mode**

Privileged EXEC

**Default**

N/A

**Usage**

Use this command to show the bfd static configurations.

**Examples**

The following example is the result of this command:

```
Switch# show bfd static configurations

```

---
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>VRF</th>
<th>LocalDiscr</th>
<th>RemoteDiscr</th>
<th>Src Ip</th>
<th>Dst Ip</th>
<th>interface</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>test1</td>
<td>single-hop</td>
<td>default</td>
<td>-</td>
<td>-</td>
<td>10.10.10.1</td>
<td>10.10.10.2</td>
<td>vlan10</td>
<td>active</td>
</tr>
<tr>
<td>test2</td>
<td>single-hop</td>
<td>test</td>
<td>-</td>
<td>-</td>
<td>9.9.9.1</td>
<td>9.9.9.2</td>
<td>vlan4094</td>
<td>active</td>
</tr>
<tr>
<td>test3</td>
<td>single-hop</td>
<td>default</td>
<td>8191</td>
<td>4294967295</td>
<td>10.10.10.1</td>
<td>10.10.10.3</td>
<td>vlan10</td>
<td>active</td>
</tr>
</tbody>
</table>

Related Commands

None

13.17.10 show bfd session

Command Purpose

Use this command to show the bfd sessions.

Command Syntax

show bfd session ( detail )
show bfd session SRC DST interface IFNAME ( detail )
show bfd session SRC DST ( detail )
show bfd session discriminator SESS ( detail )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Show session details</td>
<td>-</td>
</tr>
<tr>
<td>SRC</td>
<td>Local IPv4 address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>DST</td>
<td>Neighbor IPv4 address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IFNAME</td>
<td>BFD Interface</td>
<td>Support</td>
</tr>
<tr>
<td>discriminator SESS</td>
<td>BFD session index</td>
<td>1-4294967295</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

N/A

Usage

Use this command to show the bfd session.
Use the key word "detail" to show the detailed information.
To filter the show result, user can specify the session's source and destination address and interface.

Examples

The following example is the result of this command:

```
DUT1# show bfd session
```

Abbreviation:

LD: Local Discriminator.
RD: Remote Discriminator
S: Single hop session.
M: Multi hop session.
SD: Static Discriminator.
DD: Dynamic Discriminator
A: Admin down.
D: Down.
I: Init.
U: Up.
DUT1# show bfd session detail

<table>
<thead>
<tr>
<th>LD</th>
<th>RD</th>
<th>TYPE ST</th>
<th>UP-Time</th>
<th>Remote-Addr</th>
<th>VRF</th>
</tr>
</thead>
<tbody>
<tr>
<td>8191</td>
<td>4294967295</td>
<td>S-SD D</td>
<td>00:00:00</td>
<td>10.10.10.3</td>
<td>default</td>
</tr>
<tr>
<td>8192</td>
<td>0</td>
<td>S-DD D</td>
<td>00:00:00</td>
<td>11.11.11.2</td>
<td>yoush</td>
</tr>
<tr>
<td>8193</td>
<td>0</td>
<td>S-DD D</td>
<td>00:00:00</td>
<td>10.10.10.2</td>
<td>default</td>
</tr>
<tr>
<td>8194</td>
<td>0</td>
<td>S-DD D</td>
<td>00:00:00</td>
<td>9.9.9.2</td>
<td>test</td>
</tr>
</tbody>
</table>

Number of Sessions: 4

Related Commands

None
13.17.11 show resource bfd static configurations

**Command Purpose**
Use this command to show the resource of static bfd configurations

**Command Syntax**
show resource bfd static configurations

**Command Mode**
User EXEC

**Default**
None

**Usage**
Use this command to show the resource of static BFD configurations

**Examples**
The following example is the result of this command:
Switch# show resource bfd static configurations
Switch# show resource bfd static configurations
BFD (Static-BFD, Vrrp-BFD)
<table>
<thead>
<tr>
<th>Resource</th>
<th>Used</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFD static configuration</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Related Commands**

13.17.12 show bfd interface

**Command Purpose**
Use this command to show the IP bfd interface statues.

**Command Syntax**
show bfd interface ( IFNAME | all |

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>BFD Interface</td>
<td>Support</td>
</tr>
<tr>
<td></td>
<td></td>
<td>physical/aggregation/vlan/ ports</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC

**Default**
N/A

**Usage**
Use this command to show the IP bfd interface statues. User can show the specified interface or all interfaces.
Examples

The following example is the result of this command:

```
Switch# show bfd interface eth-0-9
```

```
Interface: eth-0-9  ifindex: 9  state: UP
Interface level configuration: NO ECHO, NO SLOW TMR
Timers in Milliseconds
  Min Tx: 1  Min Rx: 1  Multiplier: 3
----------------------------------------------------------
Number of Sessions: 2
  BFD discriminator: 8193  BFD state: DOWN
  BFD discriminator: 8191  BFD state: DOWN
```

Related Commands

None
Chapter 14 Device Management Commands

14.1 STM Commands

14.1.1 stm prefer

Command Purpose
Use the `stm prefer` Global Configuration command to configure the profile used in Switch Table Management (STM) resource allocation. You can use profile to allocate system memory to best support the features being used in your application. Use profile to approximate the maximum number of unicast MAC addresses, quality of service (QoS) access control entries (ACEs) and unicast routes. Use the no form of this command to return to the default profile.

Command Syntax
```
stm prefer (default | layer2 | layer3 | ipv6 )
no stm prefer
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Provide balance to all features</td>
<td>-</td>
</tr>
<tr>
<td>layer2</td>
<td>Provide maximum FDB entries. This profile maximizes system memory for use as a Layer 2 switch</td>
<td>-</td>
</tr>
<tr>
<td>layer3</td>
<td>Provide maximum Host Route/Indirect Route entries. You would typically use this profile for a router or aggregator in the middle of a network</td>
<td>-</td>
</tr>
<tr>
<td>ipv6</td>
<td>Unicast bias, supporting more IPv6 Ucast Routes. This profile is only existed when IPv6 feature is supported.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
System use the default profile when first boot up, this profile balance all the features.

Usage
Users must reload the switch for the configuration to take effect.

Examples
This example shows how to configure the ipv4 profile on the switch: You can verify your settings by entering the show stm prefer in privileged EXEC mode:
```
Switch# configure terminal
Switch(config)# stm prefer layer3
Switch(config)# exit
Switch# reload
```

Related Commands
```
show stm prefer
```
14.1.2 show stm prefer

Command Purpose

Use the show stm prefer privileged EXEC command to display information about the profiles that can be used to maximize system resources for a particular feature, or use the command without a keyword to display the profile in use.

Command Syntax

```
show stm prefer { default | layer2 | layer3 | ipv6 }
no stm prefer
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Provide balance to all features</td>
<td>-</td>
</tr>
<tr>
<td>layer2</td>
<td>Provide maximum FDB entries. This profile maximizes system memory for use as a Layer 2 switch</td>
<td>-</td>
</tr>
<tr>
<td>layer3</td>
<td>Provide maximum Host Route/Indirect Route entries. You would typically use this profile for a router or aggregator in the middle of a network</td>
<td>-</td>
</tr>
<tr>
<td>ipv6</td>
<td>Unicast bias, supporting more IPv6 Ucast Routes. This profile is only existed when IPv6 feature is supported.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

If you did not reload the switch after entering the stm prefer Global Configuration command, the show stm prefer privileged EXEC command displays the profile currently in use and not the newly configured profile.

The numbers displayed for each profile represent an approximate maximum number for each feature resource.

Examples

This is an example of output from the show stm prefer command, displaying the profile currently in use:

```
Switch# show stm prefer
Current profile is : default
  number of vlan instance : 1/4094
  number of unicast mac address : 0/65536
  number of multicast mac address : 0/2048
  number of blackhole mac address : 0/128
  number of max applied vlan mapping : 0/1024
  number of bfd sessions : 0/128
  number of CFM local&remote MEPs : 0/1024
  number of CFM lm : 0/256
  number of CFM lck : 0/24
  number of G8031 groups : 0/256
  number of G8032 rings : 0/256
  number of G8032 member ports : 0/256
  number of mac based vlan class : 0/512
  number of ipv4 based vlan class : 0/512
  number of ipv6 based vlan class : 0/0
```
### Related Commands

stm prefer

---

### 14.2 Syslog Commands

#### 14.2.1 clear logging buffer

**Command Purpose**
To clear messages from the logging buffer, use the `clear logging buffer` command in Privileged EXEC mode.

**Command Syntax**
```
clear logging buffer
```

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
Clear log messages in logging buffer

**Examples**
The following shows how to clear logging buffer:
```
Switch# clear logging buffer
```

**Related Commands**
show logging buffer

---

#### 14.2.2 logging alarm-trap

**Command Purpose**
To limit messages logged to the syslog servers based on severity, use the `logging alarm-trap` command in Global Configuration mode. To restore the default level, use the `no` form of this command.
Command Syntax

logging alarm-trap (enable | disable | level (high | lower | middle | minor))

no logging alarm-trap level

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enable logging traps</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>Disable logging traps</td>
<td>-</td>
</tr>
<tr>
<td>level high</td>
<td>The high alarm level</td>
<td>-</td>
</tr>
<tr>
<td>level lower</td>
<td>The lower alarm level</td>
<td>-</td>
</tr>
<tr>
<td>level middle</td>
<td>The middle alarm level</td>
<td>-</td>
</tr>
<tr>
<td>level minor</td>
<td>The minor alarm level</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

Logging trap is disabled.

Usage

A trap is an unsolicited message sent to a remote network management host. Logging traps should not be confused with SNMP traps.

Examples

The following shows how to limit messages logged to the log servers based on severity:

Switch# configure terminal
Switch(config)# logging alarm-trap enable
Switch(config)# logging alarm-trap level high

Related Commands

logging alarm-trap level middle

14.2.3 logging file

Command Purpose

To enable writing logs into files, use the logging file command in Global Configuration mode.

Command Syntax

logging file (enable | disable)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enable writing logs to file</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>Disable writing logs to file</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

Logging file is enabled

Usage

If logging file will enabled, the log will be saved to flash:/syslog every 6 hours.
Examples

The following shows how to enable logging file function:

```
Switch# configure terminal
Switch(config)# logging file enable
```

Related Commands

```
show logging
```

14.2.4 logging level file

Command Purpose

To set severity level while writing logs into files, use the logging level file command in Global Configuration mode. To return the logging to the default level, use the no form of this command.

Command Syntax

```
logging level file ( alert | critical | debug | emergency | error | information | notice | warning | SEVERITY_LEVEL )
no logging level file
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>emergency</td>
<td>System is unusable</td>
</tr>
<tr>
<td>1</td>
<td>alert</td>
<td>Immediate action needed</td>
</tr>
<tr>
<td>2</td>
<td>critical</td>
<td>Critical conditions</td>
</tr>
<tr>
<td>3</td>
<td>error</td>
<td>Error conditions</td>
</tr>
<tr>
<td>4</td>
<td>warning</td>
<td>Warning conditions</td>
</tr>
<tr>
<td>5</td>
<td>notice</td>
<td>Normal but significant conditions</td>
</tr>
<tr>
<td>6</td>
<td>information</td>
<td>Informational messages</td>
</tr>
<tr>
<td>7</td>
<td>debug</td>
<td>Debugging messages</td>
</tr>
</tbody>
</table>

SEVERITY_LEVEL Severity level 0-7

Command Mode

Global Configuration

Default

Logging file level is information.

Usage

Specifying a severity-level causes messages only at that level and numerically lower levels to files.

Examples

In the following example, the user specifies that only messages of the levels error, critical, alerts, and emergency be logged to files:

```
Switch# configure terminal
Switch(config)# logging level file 3
```

Related Commands

logging level module

14.2.5 logging buffer

Command Purpose

To set the number of logs saved in system buffer, use the logging buffer command in Global Configuration mode. To return the logging to the default value, use the no form of this command.
### Command Syntax

logging buffer **BUFFERSIZE**  
no logging buffer

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BUFFERSIZE</strong></td>
<td>logging buffer size</td>
<td>10-1000</td>
</tr>
</tbody>
</table>

### 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
```

**Related Commands**

show logging buffer

### 14.2.6 logging level module

#### Command Purpose

To set severity level, use the logging level module command in Global Configuration mode. To return the logging to the default level, use the no form of this command.

#### Command Syntax

logging level module ( alert | critical | debug | emergency | error | information | notice | warning | **SEVERITY_LEVEL** )

no logging level module

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>emergency</td>
<td>System is unusable</td>
</tr>
<tr>
<td>1</td>
<td>alert</td>
<td>Immediate action needed</td>
</tr>
<tr>
<td>2</td>
<td>critical</td>
<td>Critical conditions</td>
</tr>
<tr>
<td>3</td>
<td>error</td>
<td>Error conditions</td>
</tr>
<tr>
<td>4</td>
<td>warning</td>
<td>Warning conditions</td>
</tr>
<tr>
<td>5</td>
<td>notice</td>
<td>Normal but significant conditions</td>
</tr>
<tr>
<td>6</td>
<td>information</td>
<td>Informational messages</td>
</tr>
<tr>
<td>7</td>
<td>debug</td>
<td>Debugging messages</td>
</tr>
</tbody>
</table>

**SEVERITY_LEVEL**  
Severity level  0-7

### Command Mode

Global Configuration

**Default**

Logging file level is debugging.
Usage
Specifying a severity-level causes messages only at that level and numerically lower levels of the modules.

Examples
In the following example, the user specifies that all messages be logged:

Switch# configure terminal
Switch(config)# logging level module debug

Related Commands
logging level file

14.2.7 logging merge

Command Purpose
To enable the logging 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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enable logging mergence</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>Disable logging mergence</td>
<td>-</td>
</tr>
<tr>
<td>fifo-size SIZE</td>
<td>Set fifo size. The range is 100 to 10240, default value is 1024</td>
<td>100-10240</td>
</tr>
<tr>
<td>timeout SECONDS</td>
<td>Set timeout. The range is 1 to 300 seconds, default value is 10 seconds</td>
<td>1-300</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
Logging mergence is enabled.

Usage
The logging merge command merges all the same logs into one during a specified time range. During this time, the switch buffered these same logs. You can use the timeout keyword to set the time range, and use the fifo-size to set the buffer size.

Examples
The following shows how to enable logging merge function:

Switch# configure terminal
Switch(config)# logging merge enable

Related Commands
logging merge timeout 30

14.2.8 logging sync

Command Purpose
To synchronize log from buffer to syslog file, use the logging sync command in privileged EXEC mode.
Command Syntax
logging sync

Command Mode
Privileged EXEC

Default
None

Usage
When enabled log merge, system will merge all the same logs into one during a specified time range. During this time log will not send to logging buffer. If user wants to sync log to logging buffer, use this command. And synchronize log from buffer to syslog file.

Examples
The following shows how to enable logging sync function:
Switch# logging sync

Related Commands
logging merge enable logging sync timeout

14.2.9 logging sync timeout

Command Purpose
To set the timeout that synchronize log from buffer to syslog file. To restore to default value, use the no form of this command.

Command Syntax
logging sync timeout INTERVAL
no logging sync timeout

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>sync timeout in minutes</td>
<td>5-1440</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
360 minutes

Usage
None

Examples
The following shows how to set every 5 minutes synchronize log from buffer to syslog file:
Switch# configure terminal
Switch(config)# logging sync timeout 5

Related Commands
logging sync

14.2.10 logging operate

Command Purpose
To log the operations, and use the logging operate command in Global Configuration mode.
Command Syntax

logging operate ( enable | disable )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enable logging operations</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>Disable logging operations</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

Logging operations is disabled

Usage

If logging operate is enabled, all the CLI in configure mode or higher will be save to logger buffer.

Examples

The following shows how to enable logging operate function:

Switch# configure terminal
Switch(config)# logging operate enable

Related Commands

logging server

14.2.11 logging server

Command Purpose

To enable the logging to the remote logging servers, use the logging server command in Global Configuration mode.

Command Syntax

logging server ( enable | disable )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enable logging server</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>Disable logging server</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

Logging operations is disabled.

Usage

This command is used to send logger to a remote server.

Examples

The following shows how to use logging server command:

Switch# configure terminal
Switch(config)# logging server enable

Related Commands

logging server severity
14.2.12 logging server address

Command Purpose
To log system messages and debug output to a remote server, use the logging server address command in Global Configuration mode. To remove a specified logging server from the configuration, use the no form of this command.

Command Syntax
logging server address (mgmt-if | ) (IPV4_ADDR | IPV6_ADDR) (source-interface IFNAME | source-ip SRC_IP_ADDR )
no logging server address (mgmt-if | ) (IPV4_ADDR | IPV6_ADDR )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt-if</td>
<td>Management port</td>
<td>-</td>
</tr>
<tr>
<td>IPV4_ADDR</td>
<td>IPv4 address of the server that will receive the system logging messages</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IPV6_ADDR</td>
<td>IPv6 address of the server that will receive the system logging messages</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Name of source interface</td>
<td>All interface type</td>
</tr>
<tr>
<td>SRC_IP_ADDR</td>
<td>Source IP address</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
System logging messages are not sent to any remote server.

Usage
The logging server address command identifies a remote server (usually a device serving as a syslog server) to receive logging messages. By issuing this command more than once, you can build a list of servers that receive logging messages. If the source interface or source IP address is specified, the packet transmit will use the related IP address as source address.

Examples
In the following example, messages are logged to a server at 209.165.202.169:
Switch# configure terminal
Switch(config)# logging server address 209.165.202.169

Related Commands
logging server

14.2.13 logging server facility

Command Purpose
To configure the syslog facility in which error messages are sent, use the logging server facility command in Global Configuration mode. To revert to the default of local7, use the no form of this command.

Command Syntax
logging server facility (kern | user | mail | daemon | auth | syslog | lpr | news | uucp | cron | authpriv | ftp | FACILITY_TYPE | FACILITY_LOCAL )
no logging server facility
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>kern</td>
<td>Kernel</td>
</tr>
<tr>
<td>1</td>
<td>user</td>
<td>User</td>
</tr>
<tr>
<td>2</td>
<td>mail</td>
<td>Mail system</td>
</tr>
<tr>
<td>3</td>
<td>daemon</td>
<td>System daemon</td>
</tr>
<tr>
<td>4</td>
<td>auth</td>
<td>Authorization system</td>
</tr>
<tr>
<td>5</td>
<td>syslog</td>
<td>System log</td>
</tr>
<tr>
<td>6</td>
<td>lpr</td>
<td>Line printer system</td>
</tr>
<tr>
<td>7</td>
<td>news</td>
<td>USENET news</td>
</tr>
<tr>
<td>8</td>
<td>uucp</td>
<td>UNIX-to-UNIX</td>
</tr>
<tr>
<td>9</td>
<td>cron</td>
<td>Cron facility</td>
</tr>
<tr>
<td>10</td>
<td>authpriv</td>
<td>Authorization priv system</td>
</tr>
<tr>
<td>11</td>
<td>ftp</td>
<td>FTP system</td>
</tr>
<tr>
<td>16</td>
<td>local0</td>
<td>Reserved for locally defined messages</td>
</tr>
<tr>
<td>17</td>
<td>local1</td>
<td>Reserved for locally defined messages</td>
</tr>
<tr>
<td>18</td>
<td>local2</td>
<td>Reserved for locally defined messages</td>
</tr>
<tr>
<td>19</td>
<td>local3</td>
<td>Reserved for locally defined messages</td>
</tr>
<tr>
<td>20</td>
<td>local4</td>
<td>Reserved for locally defined messages</td>
</tr>
<tr>
<td>21</td>
<td>local5</td>
<td>Reserved for locally defined messages</td>
</tr>
<tr>
<td>22</td>
<td>local6</td>
<td>Reserved for locally defined messages</td>
</tr>
<tr>
<td>23</td>
<td>local7</td>
<td>Reserved for locally defined messages</td>
</tr>
</tbody>
</table>

**FACILITY_TYPE**

Reserved for system defined messages 0-11

**FACILITY_LOCAL**

Reserved for locally defined messages 6-23

---

**Command Mode**

Global Configuration

**Default**

Default is local4

**Usage**

None

**Examples**

The following shows how to use logging file command:

Switch# configure terminal

Switch(config)# logging server facility local3
Related Commands

logging server

14.2.14 logging server severity

Command Purpose

To set severity level while writing logs into servers, use the logging server severity command in Global Configuration mode. To revert to the default severity level, use the no form of this command.

Command Syntax

logging server severity { alert | critical | debug | emergency | error | information | notice | warning | SEVERITY_LEVEL }
no logging server severity

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 emergency</td>
<td>System is unusable</td>
<td></td>
</tr>
<tr>
<td>1 alert</td>
<td>Immediate action needed</td>
<td></td>
</tr>
<tr>
<td>2 critical</td>
<td>Critical conditions</td>
<td></td>
</tr>
<tr>
<td>3 error</td>
<td>Error conditions</td>
<td></td>
</tr>
<tr>
<td>4 warning</td>
<td>Warning conditions</td>
<td></td>
</tr>
<tr>
<td>5 notice</td>
<td>Normal but significant conditions</td>
<td></td>
</tr>
<tr>
<td>6 information</td>
<td>Informational messages</td>
<td></td>
</tr>
<tr>
<td>7 debug</td>
<td>Debugging messages</td>
<td></td>
</tr>
<tr>
<td>SEVERITY_LEVEL</td>
<td>Severity level</td>
<td>0-7</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

Logging server level is information.

Usage

This command is used to set severity level while writing logs into servers.

Examples

In the following example, the user specifies that only messages of the levels error, critical, alerts, and emergency be logged to server:

Switch# configure terminal
Switch(config)# logging server severity 3

Related Commands

logging level module
logging level file

14.2.15 logging timestamp

Command Purpose

To configure the system to apply a time-stamp to debugging messages or system logging messages, use the logging timestamps command in Global Configuration mode. To restore the default timestamp format, use the no form of this command.

Command Syntax

logging timestamp { bsd | date | iso | none | rfc3164 | rfc3339 }
no logging timestamp
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>bsd</td>
<td>BSD style (RFC 3164)</td>
<td>-</td>
</tr>
<tr>
<td>date</td>
<td>Date command style</td>
<td>-</td>
</tr>
<tr>
<td>iso</td>
<td>ISO style (RFC 3339)</td>
<td>-</td>
</tr>
<tr>
<td>none</td>
<td>No timestamp</td>
<td>-</td>
</tr>
<tr>
<td>rfc3164</td>
<td>RFC 3164 style (bsd)</td>
<td>-</td>
</tr>
<tr>
<td>rfc3339</td>
<td>RFC 3339 style (iso)</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

Default timestamp format is BSD.

**Usage**

This command is used to specify the timestamp in logger message.

**Examples**

The following shows how to set the timestamp to iso:

```
Switch# configure terminal
Switch(config)# logging timestamp iso
```

**Related Commands**

show logging

**14.2.16 show logging**

**Command Purpose**

To display the state of system logging (syslog), use the show logging command in privileged EXEC mode.

**Command Syntax**

show logging

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

The following shows how to display the configuration of the log:

```
Switch# show logging

Current logging configuration:
=================================================================================
logging buffer 500
logging timestamp date
logging file enable
logging level file warning
logging level module debug
logging server disable
```
Related Commands

logging level

14.2.17 show logging buffer

Command Purpose
To display the contents of the standard system logging buffer, use the show logging buffer command in privileged EXEC mode.

Command Syntax

```
show logging buffer [ LINES | statistics ]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LINES</td>
<td>Specify the max number of messages displayed on top, positive number means latest</td>
<td>-1000-1000</td>
</tr>
<tr>
<td></td>
<td>negative number means the oldest message displayed on top.</td>
<td></td>
</tr>
<tr>
<td>statistics</td>
<td>Display statistics of logging buffers</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

Display 20 messages when messages number is not specified. The latest message is displayed on top

Usage

None

Examples

The following shows how to use show logging buffer command:
```
Switch# show logging buffer statistics

Logging buffer statistics:
============================================================================================================
Total processed 153 entries
Total dropped 0 entries
Current have 153 entries
The latest message is:
Aug 6 16:06:44 Switch3 IMISH-6: ready to service
The oldest message is:
Aug 6 13:38:38 Switch LOGGING-5: logging starting up; version="2.0rc4"
```

Related Commands

show logging
14.3 Mirror Commands

14.3.1 monitor session destination interface

Command Purpose
Use this command to set mirror destination interface. To remove this setting, use the no form of this command.

Command Syntax
```
monitor session SESSION-ID destination interface IFNAME
no monitor session SESSION destination
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SESSION-ID</td>
<td>mirror session number</td>
<td>1-3</td>
</tr>
<tr>
<td>IFNAME</td>
<td>mirror destination interface</td>
<td>Support aggregation, physical and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tunnel interfaces</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
Same session can't configure both local destination interface and remote destination VLAN.(About the remote destination VLAN, please refer to chapter "monitor session destination remote")

Examples
This example shows how to set the mirror destination port to eth-0-1 in session 1:
```
Switch# configure terminal
Switch(config)# monitor session 1 destination interface eth-0-1
```
This example shows how to remove this setting:
```
Switch# configure terminal
Switch(config)# no monitor session 1 destination
```

Related Commands
```
monitor session SESSION-ID source interface
monitor session SESSION-ID source vlan
show monitor
```

14.3.2 monitor session destination cpu

Command Purpose
Use this command to set mirror destination of cpu. To remove this setting, use the no form of this command.

Command Syntax
```
monitor session SESSION-ID destination cpu
no monitor session SESSION-ID destination
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SESSION-ID</td>
<td>mirror session number</td>
<td>1-3</td>
</tr>
<tr>
<td>destination cpu</td>
<td>mirror destination cpu</td>
<td>-</td>
</tr>
</tbody>
</table>
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
destination
monitor session SESSION-ID source vlan
destination
show monitor

14.3.3 monitor session destination group

Command Purpose
Use this command to create mirror multi destination group and enter mirror destination group mode. To remove this setting, use the no form of this command.

Command Syntax
```
monitor session SESSION-ID destination group GROUP-ID
```
```
no monitor session SESSION-ID destination
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SESSION-ID</td>
<td>mirror session number</td>
<td>1-3</td>
</tr>
<tr>
<td>Destination group GROUP-ID</td>
<td>mirror destination group id number</td>
<td>1-32</td>
</tr>
</tbody>
</table>

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
destination
member
show monitor
14.3.4 member

Command Purpose

Use this command to add a group member mirror destination interface for a mirror destination group. To remove this setting, use the no form of this command.

Command Syntax

member IFPHYSICAL

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFPHYSICAL</td>
<td>mirror destination interface</td>
<td>Support physical ports</td>
</tr>
</tbody>
</table>

Command Mode

Mirror Destination Group Configuration

Default

None

Usage

The destination interface only can be physical port. It can be neither VLAN interface nor Aggregator interface. Same session can't configure both local destination interface and multi-destination interface.

Examples

This example shows how to add the mirror destination eth-0-1 to group of multi-destination session:

```
Switch# configure terminal
Switch(config)# monitor session 1 destination group 1
Switch(config-monitor-d-group)# member eth-0-1
```

This example shows how to remove this setting:

```
Switch# configure terminal
Switch(config)# monitor session 1 destination group 1
Switch(config-monitor-d-group)# no member eth-0-1
```

Related Commands

monitor session SESSION-ID source interface
monitor session SESSION-ID destination group GROUP-ID
show monitor

14.3.5 monitor session source interface

Command Purpose

Command Syntax

monitor session SESSION-ID source interface interface ( both | tx | rx )
no monitor session SESSION-ID source interface IFNAME ( both | tx | rx )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SESSION-ID</td>
<td>mirror session number</td>
<td>1-3</td>
</tr>
<tr>
<td>source interface IFNAME</td>
<td>mirror source interface</td>
<td>Support aggregation and physical interfaces</td>
</tr>
<tr>
<td>both</td>
<td>monitor received and transmitted traffic on that interface</td>
<td>-</td>
</tr>
<tr>
<td>rx</td>
<td>monitor received traffic only on that interface</td>
<td>-</td>
</tr>
<tr>
<td>tx</td>
<td>monitor transmitted traffic only on that interface</td>
<td>-</td>
</tr>
</tbody>
</table>
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-0-1
This example shows how to remove this setting:
Switch# configure terminal
Switch(config)# no monitor session 1 source interface eth-0-1

Related Commands
monitor session SESSION-ID destination
show monitor

14.3.6 monitor session source vlan

Command Purpose
Use this command to set mirror source vlan.
To remove this setting, use the no form of this command.

Command Syntax
monitor session SESSION-ID source vlan VLAN-ID (both | tx | rx)
no monitor session SESSION-ID source vlan VLAN-ID (both | tx | rx)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SESSION-ID</td>
<td>mirror session number</td>
<td>1-3</td>
</tr>
<tr>
<td>VLAN-ID</td>
<td>the source vlan id to be mirrored</td>
<td>1-4094</td>
</tr>
<tr>
<td></td>
<td>monitor received and transmitted traffic on that interface</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>monitor received traffic only on that interface</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>monitor transmitted traffic only on that interface</td>
<td>-</td>
</tr>
</tbody>
</table>

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
```

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)# vlan database
Switch(config-vlan)# no vlan 2
Switch(config-vlan)# exit
```

Related Commands

- monitor session destination
- show monitor
- vlan database
- vlan VLAN-ID
- interface vlan VLAN-ID

14.3.7 monitor session source cpu

Command Purpose

Use this command to set mirror source cpu
To remove this setting, use the no form of this command.

Command Syntax

```
monitor session SESSION-ID source cpu ( both | tx | rx )
no monitor session SESSION-ID source cpu ( both | tx | rx )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SESSION-ID</td>
<td>mirror session number</td>
<td>1-3</td>
</tr>
<tr>
<td>cpu</td>
<td>set cpu to be mirrored</td>
<td>-</td>
</tr>
<tr>
<td>both</td>
<td>monitor received and transmitted traffic on that interface</td>
<td>-</td>
</tr>
<tr>
<td>rx</td>
<td>monitor received traffic only on that interface</td>
<td>-</td>
</tr>
<tr>
<td>tx</td>
<td>monitor transmitted traffic only on that interface</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None
Usage

If the parameter for direction (both|tx|rx) is not specified, the default value is both.
Mirror source cpu can only be configured in session 1.

Examples

This example shows how to set the mirror source to cpu in session 1:
Switch# configure terminal
Switch(config)# monitor session 1 source cpu both

This example shows how to set the mirror source to cpu in session 1 to monitor received traffic only:
Switch# configure terminal
Switch(config)# monitor session 1 source cpu rx

This example shows how to set the mirror source to cpu in session 1 to monitor transmitted traffic only:
Switch# configure terminal
Switch(config)# monitor session 1 source cpu tx

This example shows how to remove this setting:
Switch# configure terminal
Switch(config)# no monitor session 1 source cpu both

Related Commands

monitor session destination
show monitor

14.3.8 monitor session destination 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SESSION-ID</td>
<td>mirror session number</td>
<td>1-3</td>
</tr>
<tr>
<td>VLAN-ID</td>
<td>Remote mirror destination VLAN id</td>
<td>2-4094</td>
</tr>
<tr>
<td>IFNAME</td>
<td>the out-going interface for mirrored packets</td>
<td>Support physical interface</td>
</tr>
</tbody>
</table>

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
dl vlan VLAN-ID

14.3.9 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 fspan(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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC</td>
<td>mac address</td>
<td>mac address in HHHH. HHHH. HHHH format</td>
</tr>
<tr>
<td>MASK</td>
<td>mac address mask</td>
<td>mac address mask in HHHH. HHHH. HHHH format</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

Mac escape is used for remote mirror. It will not affect the result of local mirror. If a Mac escape entry is set, the packet with this Mac destination can not be mirrored in remote mirror. Command "no monitor mac escape " should delete the specified entry. Command "no monitor mac escape" should delete all entries.

Examples

This example shows how to set the mirror mac escape:
Switch# configure terminal
Switch(config)# monitor mac escape 00cc.1122.3344 ffff.ffff.0000
This example shows how to remove this setting:
Switch# configure terminal
Switch(config)# no monitor mac escape 00cc.1122.3344 ffff.ffff.0000

Related Commands

monitor session SESSION-ID destination remote
14.3.10 show monitor

Command Purpose
Use this command to show the information about monitor.

Command Syntax
show monitor ( session SESSION-ID )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SESSION-ID</td>
<td>mirror session number</td>
<td>1-3</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
If session id is not specified, any configured sessions should be shown.

Examples
This example shows how to display the information about monitor:
DUT1# show monitor
session 1

Session 1
----------
Status     : Valid
Type       : Local Session
Source Ports:
  Receive Only:
  Transmit Only:
  Both         : eth-0-2
Source VLANs:
  Receive Only:
  Transmit Only:
  Both
Destination Port : eth-0-1

Related Commands
monitor session SESSION-ID source interface
monitor session SESSION-ID source vlan
monitor session SESSION-ID source cpu
monitor session SESSION-ID destination interface
monitor session SESSION-ID destination remote
monitor session SESSION-ID destination cpu

14.3.11 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

14.3.12 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

14.3.13 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIZE</td>
<td>buffer size in packets</td>
<td>1-1000, unit:packet</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

Default 1000

Usage

The mirror cpu buffer can store up to 1000 packets and the default value is 1000.

Examples

This example shows how to set mirror cpu buffer size:
Switch# configure terminal
Switch(config)# monitor cpu set packet buffer 50

Related Commands

show monitor cpu packet buffer size

14.3.14 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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>start</td>
<td>start capture</td>
<td>-</td>
</tr>
<tr>
<td>stop</td>
<td>stop capture</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

Stop

Usage

When start capturing packet, the cpu mirror packets will be written in a text file and the file name is assigned by system. The text file is stored in the directory of flash/mirror/

Examples

This example shows how to start cpu capturing packets in a text file:
Switch# configure terminal
Switch(config)# monitor cpu capture packet start
This example shows how to stop cpu capturing packets in a text file:
Switch# configure terminal
Switch(config)# monitor cpu capture packet stop

Related Commands

pcap convert FILENAMEA FILENAMEB
14.3.15  monitor cpu capture strategy

Command Purpose
Use this command to set the strategy of capturing packets.

Command Syntax
monitor cpu capture strategy (replace | drop)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>replace</td>
<td>the oldest packet would be replaced by the latest packet when cpu mirror memory buffer is full</td>
<td>-</td>
</tr>
<tr>
<td>drop</td>
<td>the latest packet would be discarded when cpu mirror memory buffer is full</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
Replace

Usage
None

Examples
This example shows how to set cpu capture strategy as replace:
Switch# configure terminal
Switch(config)# monitor cpu capture strategy replace
This example shows how to set cpu capture strategy as drop:
Switch# configure terminal
Switch(config)# monitor cpu capture strategy drop

Related Commands
show monitor cpu capture strategy

14.3.16  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)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>show all of mirror cpu packets in memory</td>
<td>-</td>
</tr>
<tr>
<td>PACKET-ID</td>
<td>show the mirror cpu packets of user specifying</td>
<td>1-1000</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC
### 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

**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>)
Examples

This example shows how to show the mirror cpu buffer size in memory:

```
Switch(config)# show monitor cpu packet buffer-size
```

Related Commands

monitor cpu set packet buffer <1-1000>

### 14.3.19 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)

### 14.4 Device Management Commands

#### 14.4.1 Temperature

**Command Purpose**

To specify the system temperature monitor threshold.

**Command Syntax**

```
temperature LOW/HIGH/CRITICAL
no temperature
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOW</td>
<td>Low alarm temperature degree Celsius</td>
<td>45-50, unit:degree Celsius</td>
</tr>
<tr>
<td>HIGH</td>
<td>High alarm temperature degree Celsius</td>
<td>50-85, unit:degree Celsius</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>Critical alarm temperature degree Celsius</td>
<td>55-100, unit:degree Celsius</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

---

www.fs.com
Default

The default threshold is low temperature 5, high temperature 75, and critical temperature 90.

Usage

The unit for temperature is centigrade.
The critical temperature must higher than high temperature 5 Celsius degrees.
The high temperature must higher than low temperature 5 Celsius degrees.

Examples

This example shows how to specify the temperature thresholds:
Switch# configure terminal
Switch(config)# temperature 5 70 90

Related Commands

show environment

14.4.2 show environment

Command Purpose

Use this command to show the hardware environment information.

Command Syntax

show environment (slot ID | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>The ID of stack member.</td>
<td>1-29</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display hardware environment information:
Switch# show environment

Fan tray status:
Index  Status
1     PRESENT
FanIndex  Status SpeedRate Mode
1-1  OK  30%  Auto
1-2  OK  30%  Auto
1-3  OK  30%  Auto

Power status:
Index  Status  Power  Type  Alert
1     PRESENT  OK  AC  NO
2     ABSENT  -  -  -

Sensor status (Degree Centigrade):
Index  Temperature  Lower_alarm  Upper_alarm Critical_limit
1     64  5  75  90

Related Commands

Temperature
14.4.3 boot system

Command Purpose

Use this command to specify the system image that the switch loads at startup.

Command Syntax

boot system (GFLASHFILE | tftp: mgmt-if IP_ADDR GTFTPFLIE)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GFLASHFILE</td>
<td>The file name that will be used to load at startup</td>
<td>File path and name on the flash</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>The tftp server IP address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>tftp: mgmt-if</td>
<td>Use management port</td>
<td></td>
</tr>
<tr>
<td>GTFTPFLIE</td>
<td>The file name that will be used to load at startup</td>
<td>File name on the tftp server</td>
</tr>
</tbody>
</table>

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 ulimage.r

Related Commands

None

14.4.4 show transceiver

Command Purpose

Use this command to show the transceiver information.

Command Syntax

show transceiver (interface | } ( detail | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Specify the physical interface</td>
<td>-</td>
</tr>
<tr>
<td>detail</td>
<td>Show detail include DDM information</td>
<td>-</td>
</tr>
</tbody>
</table>

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.
The threshold values are calibrated.

<table>
<thead>
<tr>
<th>Port</th>
<th>Temperature (Celsius)</th>
<th>High Alarm Threshold (Celsius)</th>
<th>High Warn Threshold (Celsius)</th>
<th>Low Warn Threshold (Celsius)</th>
<th>Low Alarm Threshold (Celsius)</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-1-2</td>
<td>25.92</td>
<td>95.00</td>
<td>90.00</td>
<td>-20.00</td>
<td>-25.00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Voltage (Volts)</th>
<th>High Alarm Threshold (Volts)</th>
<th>High Warn Threshold (Volts)</th>
<th>Low Warn Threshold (Volts)</th>
<th>Low Alarm Threshold (Volts)</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-1-2</td>
<td>3.32</td>
<td>3.80</td>
<td>3.70</td>
<td>2.90</td>
<td>2.80</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Current (milliamperes)</th>
<th>High Alarm Threshold (mA)</th>
<th>High Warn Threshold (mA)</th>
<th>Low Warn Threshold (mA)</th>
<th>Low Alarm Threshold (mA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-1-2</td>
<td>6.41</td>
<td>20.00</td>
<td>18.00</td>
<td>1.00</td>
<td>0.50</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Optical Transmit Power (dBm)</th>
<th>High Alarm Threshold (dBm)</th>
<th>High Warn Threshold (dBm)</th>
<th>Low Warn Threshold (dBm)</th>
<th>Low Alarm Threshold (dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-1-2</td>
<td>-2.41</td>
<td>2.01</td>
<td>1.00</td>
<td>-6.99</td>
<td>-7.96</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Optical Receive Power (dBm)</th>
<th>High Alarm Threshold (dBm)</th>
<th>High Warn Threshold (dBm)</th>
<th>Low Warn Threshold (dBm)</th>
<th>Low Alarm Threshold (dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-1-2</td>
<td>-12</td>
<td>-</td>
<td>1.00</td>
<td>0.00</td>
<td>-19.00</td>
</tr>
</tbody>
</table>

Related Commands
None

14.4.5 update bootrom

Command Purpose
Use this command to update bootrom image.

Command Syntax
update bootrom (flash | udisk)
### Command: update bootrom

**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

### Command: show reboot-info

**Command Purpose**
Use this command to show reboot info.

**Command Syntax**
show reboot-info (slot | )

**Parameter** | **Parameter Description** | **Parameter Value**
---|---|---
ID | The ID of stack member. | 1-29

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**

<table>
<thead>
<tr>
<th>Reboot Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POWER</td>
<td>Power outages</td>
</tr>
<tr>
<td>MANUAL</td>
<td>Cli &quot;reboot/reload&quot; undersystem</td>
</tr>
<tr>
<td>HIGH-TMPR</td>
<td>Reboot for abnormal high temperature</td>
</tr>
<tr>
<td>BHMDOG</td>
<td>BHM watchdog, monitor functional module</td>
</tr>
<tr>
<td>LCMDOG</td>
<td>LCM watchdog, monitor each LC</td>
</tr>
<tr>
<td>SCHEDULE</td>
<td>Schedule reboot</td>
</tr>
<tr>
<td>SNMP-RELOAD</td>
<td>SNMP reboot</td>
</tr>
<tr>
<td>HALFAIL</td>
<td>Reboot for HAGT communicate with HSRV failed, need stack enable</td>
</tr>
<tr>
<td>ABNORMAL</td>
<td>Unusual reboot, include reboot under shell</td>
</tr>
<tr>
<td>CTCINTR</td>
<td>Button reboot</td>
</tr>
<tr>
<td>LCATTACH</td>
<td>Reboot for LC attach CHSM failed</td>
</tr>
<tr>
<td>OTHER</td>
<td>Other reboot</td>
</tr>
<tr>
<td>OTHER</td>
<td>Other reboot</td>
</tr>
</tbody>
</table>
Examples

This example shows how to show reboot-info:

Switch# show reboot-info

<table>
<thead>
<tr>
<th>Times</th>
<th>Reboot Type</th>
<th>Reboot Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MANUAL</td>
<td>2016/09/08 15:14:41</td>
</tr>
<tr>
<td>2</td>
<td>MANUAL</td>
<td>2016/09/08 14:23:31</td>
</tr>
<tr>
<td>3</td>
<td>MANUAL</td>
<td>2000/01/01 00:00:01</td>
</tr>
<tr>
<td>4</td>
<td>HIGH-TMPR</td>
<td>2000/01/01 01:01:40</td>
</tr>
<tr>
<td>5</td>
<td>MANUAL</td>
<td>2000/01/01 00:00:17</td>
</tr>
<tr>
<td>6</td>
<td>ABNORMAL</td>
<td>1959/11/25 17:44:24</td>
</tr>
<tr>
<td>7</td>
<td>MANUAL</td>
<td>1959/11/26 14:51:37</td>
</tr>
<tr>
<td>8</td>
<td>MANUAL</td>
<td>1959/11/28 09:04:35</td>
</tr>
<tr>
<td>9</td>
<td>MANUAL</td>
<td>2016/09/12 09:44:53</td>
</tr>
<tr>
<td>10</td>
<td>MANUAL</td>
<td>2000/01/01 00:00:01</td>
</tr>
</tbody>
</table>

Related Commands

None

14.5 Bootrom Commands

14.5.1 Version

Command Purpose

Use the version command to show the Bootrom version information.

Command Syntax

Version

Command Mode

BootRom CLI

Default

None

Usage

None

Examples

This example shows how to show the U-boot version:

bootrom:> version

U-Boot 2013.01-svn11932 (Sep 01 2015 - 17:12:25) - V8.1.0
powerpc-fsl_networking-linux-gnu-gcc (GCC) 4.7.2
GNU ld (GNU Binutils) 2.23.1.20121113

Related Commands

None

14.5.2 Setenv

Command Purpose

Use this command to set Bootrom environment variables.

Command Syntax

setenv (ipaddr | serverip IP_ADDR | bootcmd boot arguments )
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>Local device or tftp server IP address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>boot arguments</td>
<td>Boot form flash or tftp server</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

BootRom CLI

**Default**

None

**Usage**

None

**Examples**

This example shows how to set Switch IP address as environment variables:

```bash
bootrom: setenv ipaddr 10.10.29.48
```

This example shows how to set TFTP server IP address as environment variables:

```bash
bootrom: setenv serverip 10.10.29.160
```

This example shows how to set boot command as environment variables:

```bash
bootrom: setenv bootcmd boot_flash OS-ma-v3.0.1.it.r.bin
```

**Related Commands**

None

14.5.3 Saveenv

**Command Purpose**

Use the saveenv command to save the Bootrom environment variables to persistent storage.

**Command Syntax**

Saveenv

**Command Mode**

Saveenv

BootRom CLI

**Default**

None

**Usage**

None

**Examples**

This example shows how to save the Bootrom environment variables:

```bash
bootrom: saveenv
```

**Related Commands**

Printenv

14.5.4 Printenv

**Command Purpose**

Use the printenv command to show the U-boot environment variables.
Command Syntax

Printenv

Command Mode

BootRom CLI

Default

None

Usage

None

Examples

This example shows how to show the Bootrom environment variables:

```
bootrom:> printenv

baudrate=115200
bootargs=bootimage=ulimage console=ttys0,115200 cache-sram=0xfff00000,0x10000
bootcmd=boot_tftp switchOS-v6.2.27.r.bin
bootdelay=10
consoledev=ttys0
ethact=ETSEC2
ethaddr=00:00:00:00:01:02
ethprime=ETSEC2
fileaddr=1000000
filesize=2126519
gatewayip=10.10.39.254
ipaddr=10.10.39.123
loadaddr=1000000
mtddevname=uboot-env
mtddevnum=0
mtdids=nand0=nand
partition=nand0,0
serial#=E132GD153002
serverip=10.10.38.160
stderr=serial
stdin=serial
stdout=serial

Environment size: 4720/8188 bytes
```

Related Commands

Setenv

14.5.5 Reset

Command Purpose

Use the reset command to perform RESET of the CPU.

Command Syntax

Reset

Command Mode

BootRom CLI

Default

None

Usage

None
Examples

This example shows how to RESET the CPU in Bootrom:

```
bootrom> reset
```

Related Commands

Saveenv

14.5.6 Ping

Command Purpose

Use the ping command to send ICMP ECHO_REQUEST to network host.

Command Syntax

```
ping IP_ADDR
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>remote host IP address</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

Command Mode

BootRom CLI

Default

None

Usage

None

Examples

This example shows how to use ping command in Bootrom mode:

```
Bootrom> ping 10.10.38.160
```

Using FM1@DTSEC3 device

host 10.10.38.160 is alive

Related Commands

Saveenv

14.5.7 Ctls

Command Purpose

Use the ls command to list files in a directory (default is `/`).

Command Syntax

Ctls

Command Mode

BootRom CLI

Default

None

Usage

None
Examples

This example shows how to list files in a directory (default is `/`):

```
Bootrom:/>ctcls
```

```
Examples

This example shows how to boot system from TFTP server:

```
bootrom:/>boot_tftp OS-ma-v3.0.1.it.r.bin
```
14.5.9 boot_tftp_nopass

Command Purpose
Use the boot_tftp_nopass command to boot system through the specified system image from TFTP server with default configuration.

Command Syntax
boot_tftp_nopass IMAGE_NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMAGE_NAME</td>
<td>Image name of tftp server</td>
<td>-</td>
</tr>
</tbody>
</table>

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.itr.bin
```

Related Commands
None

14.5.10 boot_flash

Command Purpose
Use the boot_flash command to boot system through the specified image or default image in the flash.

Command Syntax
boot_flash IMAGE_NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMAGE_NAME</td>
<td>Image name in flash</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
BootRom CLI

Default
None

Usage
None

Examples
This example shows how to boot system through the specify image in the flash:
```
bootrom:~> boot_flash
```

Related Commands
None
14.5.11 boot\_flash\_nopass

**Command Purpose**

Use the `boot_flash_nopass` command to boot system through the specify image or default image in the flash with default configuration.

**Command Syntax**

`boot_flash_nopass IMAGE_NAME`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMAGE_NAME</td>
<td>Image name in flash</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

BootRom CLI

**Default**

None

**Usage**

None

**Examples**

This example shows how to boot system through the specify image in the flash with default configuration:

```
bootrom:~> boot_flash_nopass /boot/OS-ma-v3.0.1.it.r.bin
Do you want to revert to the default config file? [Y|N|E]: Y
```

**Related Commands**

None

14.5.12 upgrade\_uboot

**Command Purpose**

Use the `upgrade_uboot` command to upgrade the U-boot image from TFTP server.

**Command Syntax**

`upgrade_uboot IMAGE_NAME`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMAGE_NAME</td>
<td>Image name form tftp server</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

BootRom CLI

**Default**

None

**Usage**

None

**Examples**

This example shows how to upgrade the Bootrom image from TFTP server:

```
bootrom:~> upgrade_uboot u-boot.bin
```

**Related Commands**

None
14.6 Bootup Diagnostic Commands

14.6.1 diagnostic bootup level

Command Purpose
Use this command to set bootup diagnostic level of next Switch reboot.

Command Syntax
```
diagnostic bootup level ( minimal | complete )
no diagnostic bootup level
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>minimal</td>
<td>Minimal bootup level test</td>
<td>-</td>
</tr>
<tr>
<td>complete</td>
<td>Complete bootup level test</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
None

Examples
This example shows how to set bootup diagnostic level:
```
Switch# configure terminal
Switch(config)# diagnostic bootup level minimal
```

Related Commands
None

14.6.2 show diagnostic bootup level

Command Purpose
Use this command to show bootup diagnostic level.

Command Syntax
```
show diagnostic bootup level
```

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to show bootup diagnostic level:
```
Switch# show diagnostic bootup level
```

The current running bootup diag level is complete
The next running bootup diag level is complete
Related Commands

None

14.6.3  show diagnostic bootup result

Command Purpose

Use this command to show bootup diagnostic result.

Command Syntax

show diagnostic bootup result ( detail | ) ( slot ID | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Detailed information</td>
<td>-</td>
</tr>
<tr>
<td>ID</td>
<td>The ID of stack member.</td>
<td>1-29</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to show bootup diagnostic level:

```
Switch# show diagnostic bootup result detail
#########################################################
<table>
<thead>
<tr>
<th>Item Name</th>
<th>Attribute</th>
<th>Result</th>
<th>Time(usec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EPLD TEST</td>
<td>C</td>
<td>Pass</td>
<td>57</td>
</tr>
<tr>
<td>EEPROM0 TEST</td>
<td>C</td>
<td>Pass</td>
<td>101262</td>
</tr>
<tr>
<td>PHY TEST</td>
<td>C</td>
<td>Pass</td>
<td>1161</td>
</tr>
<tr>
<td>FAN TEST</td>
<td>C</td>
<td>Pass</td>
<td>4668</td>
</tr>
<tr>
<td>SENSOR TEST</td>
<td>C</td>
<td>Pass</td>
<td>5472</td>
</tr>
<tr>
<td>PSU TEST</td>
<td>C</td>
<td>Pass</td>
<td>1370</td>
</tr>
<tr>
<td>L2 UCAST FUNC TEST</td>
<td>C</td>
<td>Pass</td>
<td>40126</td>
</tr>
</tbody>
</table>
```

Related Commands

None

14.7  SmartConfig Commands

14.7.1  smart-config

Command Purpose

To config smartconfig function, use the smart-config command in global configuration mode.

Command Syntax

```
smart-config ( initial-switch-deployment | hostname-prefix )
nosmart-config ( initial-switch-deployment | hostname-prefix )
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>initial-switch-deployment</td>
<td>Enable initial switch automatically</td>
<td>-</td>
</tr>
<tr>
<td>hostname-prefix</td>
<td>Enable hostname prefix</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

Initial-switch-deployment and hostname-prefix is enabled.

**Usage**

None

**Examples**

The following example shows how to enable smartconfig function:

```
Switch# configure terminal
Switch(config)# smart-config initial-switch-deployment
```

The following example shows how to disable smartconfig function:

```
Switch# configure terminal
Switch(config)# no smart-config initial-switch-deployment
```

**Related Commands**

- ip address dhcp
- show smart-config config

### 14.7.2 show smart-config config

**Command Purpose**

To show configuration of smart-config, use the show smart-config configuration command in privileged EXEC mode.

**Command Syntax**

```
show smart-config config
```

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

The following example shows how to display configuration of smart-config:

```
Switch# show smart-config config
Smart-Config config:
  initial-switch-deployment: on
  hostname-prefix: on
  Send log message to console: on
```

**Related Commands**

- ip address dhcp
- smart-config

www.fs.com
14.8 Debian Commands

14.8.1 Bash

Command Purpose
To enter into debian shell mode used bash command in privileged EXEC mode.

Command Syntax
Bash

Command Mode
Privileged EXEC

Default
None

Usage
Can only be used in debian image.

Examples
This example shows how to entry into debian shell mode:
Switch# bash
switch@Switch:~$

Related Commands
None

14.8.2 show debian-version

Command Purpose
To show debian version information used show debian-version command in privileged EXEC mode.

Command Syntax
show debian-version

Command Mode
Privileged EXEC

Default
None

Usage
Can only be used in debian image.

Examples
This example shows how to display debian version information:
Switch# show debian-version
Debian version is 8.11

Related Commands
None
Chapter 15 Network Management Commands

15.1 Network Diagnosis Commands

15.1.1 ping

Command Purpose
The switch supports IP ping, which you can use to test connectivity to remote hosts. Ping sends an echo request packet to an address and waits for a reply. Ping returns one of these responses:
- Normal response- The normal response (hostname is alive) occurs in 1 to 10 seconds, depending on network traffic.
- Destination does not respond- If the host does not respond, a no-answer message is returned.
- Unknown host- If the host does not exist, an unknown host message is returned.
- Destination unreachable- If the default gateway cannot reach the specified network, a destination-unreachable message is returned.
- Network or host unreachable- If there is no entry in the route table for the host or network, a network or host unreachable message is return.

Command Syntax
```
ping (ip | mgmt-if) WORD
ping (vrf WORD | ) [-a WORD] [-si IFNAME] [-m INTERVAL | -c COUNT | -s DATASIZE | -f | -tos TTL | -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 | )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a WORD</td>
<td>Select source IP address, the default is the IP address of the output interface</td>
<td>-</td>
</tr>
<tr>
<td>-si IFNAME</td>
<td>Set the specified interface as the source interface of ping packet</td>
<td>Support physical/aggregation/loopback/tunnel/vlan ports</td>
</tr>
<tr>
<td>ip</td>
<td>Public network IPv4 echo</td>
<td>-</td>
</tr>
<tr>
<td>vrf WORD</td>
<td>VPN Routing/Forwarding instance</td>
<td>Up to 15 characters</td>
</tr>
<tr>
<td>mgmt-if</td>
<td>Management interface</td>
<td>-</td>
</tr>
<tr>
<td>WORD</td>
<td>Ping destination IPv4 or IPv6 address or hostname</td>
<td>-</td>
</tr>
<tr>
<td>ipv6</td>
<td>Public network IPv6 echo</td>
<td>-</td>
</tr>
<tr>
<td>interface</td>
<td>Outgoing interface for LinkLocal address/host</td>
<td>-</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Interface's name</td>
<td>Support physical/aggregation/loopback/tunnel/vlan ports</td>
</tr>
<tr>
<td>-m INTERVAL</td>
<td>specify interval for sending ping packets</td>
<td>10-10000 millisecond</td>
</tr>
<tr>
<td>-c COUNT</td>
<td>specify the number of ping packets</td>
<td>1-4294967295</td>
</tr>
<tr>
<td>-s DATASIZE</td>
<td>specify the data size of ping packet</td>
<td>20-9600 bytes</td>
</tr>
<tr>
<td>-f</td>
<td>specify the Don’t Fragment flag in packet</td>
<td>-</td>
</tr>
<tr>
<td>-tos TTL</td>
<td>Specify the packet tos value</td>
<td>0-255</td>
</tr>
<tr>
<td>-h TTL</td>
<td>specify the TTL value in ping packet</td>
<td>1-255</td>
</tr>
<tr>
<td>-tc TC</td>
<td>specify the Traffic Class value in ipv6 ping packet</td>
<td>0-255</td>
</tr>
<tr>
<td>-h HL</td>
<td>specify the Hop Limit value in ipv6 ping packet</td>
<td>1-255</td>
</tr>
<tr>
<td>-t TIMEOUT</td>
<td>specify the timeout value to wait for replay packet</td>
<td>0-65535 millisecond. only support multiple of 1000</td>
</tr>
</tbody>
</table>
**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

This example shows how to ping a host from management interface:

```
Switch# ping mgmt-if 10.10.29.247
PING 10.10.29.247 (10.10.29.247) 56(84) bytes of data.
64 bytes from 10.10.29.247: icmp_seq=1 ttl=64 time=0.194 ms
64 bytes from 10.10.29.247: icmp_seq=2 ttl=64 time=0.131 ms
64 bytes from 10.10.29.247: icmp_seq=3 ttl=64 time=0.134 ms
64 bytes from 10.10.29.247: icmp_seq=4 ttl=64 time=0.121 ms
64 bytes from 10.10.29.247: icmp_seq=5 ttl=64 time=0.135 ms
--- 10.10.29.247 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.121/0.143/0.194/0.025 ms
```

**Related Commands**

Traceroute

**15.1.2 traceroute**

**Command Purpose**

You can use IP traceroute to identify the path that packets take through the network on a hop-by-hop basis. The command output displays all network layer (Layer 3) devices, such as routers, that the traffic passes through on the way to the destination.

Your switches can participate as the source or destination of the traceroute privileged EXEC command and might or might not appear as a hop in the traceroute command output. If the switch is the destination of the traceroute, it is displayed as the final destination in the traceroute output. Intermediate switches do not show up in the traceroute output if they are only bridging the packet from one port to another within the same VLAN. However, if the intermediate switch is a multilayer switch that is routing a particular packet, this switch shows up as a hop in the traceroute output.

The traceroute privileged EXEC command uses the Time To Live (TTL) field in the IP header to cause routers and servers to generate specific return messages. Traceroute starts by sending a User Datagram Protocol (UDP) datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends back an Internet Control Message Protocol (ICMP) time-to-live-exceeded message to the sender. Traceroute determines the address of the first hop by examining the source address field of the ICMP time-to-live-exceeded message.

**Command Syntax**

```
traceroute (ip | vrf WORD | mgmt-if |) WORD
traceroute (vrf WORD |) ipv6 WORD
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a</td>
<td>Select source IP address, the default is the IP address of the output interface</td>
<td>-</td>
</tr>
<tr>
<td>-si</td>
<td>Set the specified interface as the source interface of traceroute packet</td>
<td>-</td>
</tr>
<tr>
<td>ip</td>
<td>Public network IPv4 echo</td>
<td>-</td>
</tr>
<tr>
<td>ipv6</td>
<td>Public network IPv6 echo</td>
<td>-</td>
</tr>
<tr>
<td>vrf WORD</td>
<td>VPN Routing/Forwarding instance</td>
<td>-</td>
</tr>
<tr>
<td>mgmt-if</td>
<td>Management interface</td>
<td>-</td>
</tr>
<tr>
<td>WORD</td>
<td>Destination IP address or hostname</td>
<td>-</td>
</tr>
</tbody>
</table>
Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
The following example is sample dialog from the traceroute command using default values:

```
Switch# traceroute 1.1.1.2
traceroute to 1.1.1.2 (1.1.1.2), 30 hops max, 38 byte packets
   1  1.1.1.2 (1.1.1.2)   108.129 ms   99.313 ms   94.720 ms
```

Related Commands
Ping

15.2 NTP Commands

15.2.1 ntp ace

Command Purpose
To create the Access Control Entries (ACE) of a NTP server/peer, use the ntp ace command in global configuration mode. To remove the ace, use the no form of this command.

Command Syntax
```
ntp ace ( IP_ADDR | HOSTNAME ) ( mask MASK_LENGTH ) ( version | kod | ignore | noquery | nomodify | notrap | noserve | nopeer | notrust | limited | none )
no ntp ace ( IP_ADDR | HOSTNAME ) ( mask MASK ) ( version | kod | ignore | noquery | nomodify | notrap | noserve | nopeer | notrust | limited | none )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>IP address of the time server or peer</td>
<td>IPv4 Address, exclude 127.0.0.1 &amp; 0.0.0.0</td>
</tr>
<tr>
<td>HOSTNAME</td>
<td>Name of the time server or peer</td>
<td>Up to 256 characters</td>
</tr>
<tr>
<td>MASK_LENGTH</td>
<td>Specify network mask length of the address</td>
<td>1-32</td>
</tr>
<tr>
<td>MASK</td>
<td>Specify network mask of the address</td>
<td>In IPv4 Address format</td>
</tr>
<tr>
<td>version</td>
<td>Ignore these hosts if not the current NTP version</td>
<td>-</td>
</tr>
<tr>
<td>kod</td>
<td>If access is denied, send a kiss-of-death packet</td>
<td>-</td>
</tr>
<tr>
<td>ignore</td>
<td>Ignore all packets from host that match this entry</td>
<td>-</td>
</tr>
<tr>
<td>noquery</td>
<td>Ignore all NTP mode 6 and 7 packets from the source, time service is not affected</td>
<td>-</td>
</tr>
<tr>
<td>nomodify</td>
<td>Ignore all NTP mode 6 and 7 packets which attempt to modify the state of the server</td>
<td>-</td>
</tr>
<tr>
<td>notrap</td>
<td>Decline to provide mode 6 control message trap service to matching hosts</td>
<td>-</td>
</tr>
<tr>
<td>noserve</td>
<td>Ignore NTP packets whose mode is other than 6 or 7</td>
<td>-</td>
</tr>
</tbody>
</table>
Parameter | Parameter Description | Parameter Value
--- | --- | ---
nopeer | Provide stateless time service to polling hosts, but do not allocate peer memory resources | -
notrust | Treat these hosts normally in other respects, but never use them as synchronization sources | -
limited | These hosts are subject to limitation of number of clients from the same net | -
none | No limit | -

**Command Mode**
Global Configuration

**Default**
None

**Usage**
Use this command if you want to allow the system to synchronize with the specified server. The server will not synchronize to this machine.

**Examples**
The following example shows how to create an ACE for 1.1.1.1:
Switch# configure terminal
Switch(config)# ntp ace 1.1.1.1 version

**Related Commands**
show ntp

15.2.2 ntp authentication

**Command Purpose**
To enable NTP authentication, use the ntp authentication enable command. To disable the NTP authentication, use the ntp authentication disable command.

**Command Syntax**
ntp authentication (enable | disable )

Parameter | Parameter Description | Parameter Value
--- | --- | ---
enable | Enable NTP authentication | -
disable | Disable NTP authentication | -

**Command Mode**
Global Configuration

**Default**
None

**Usage**
When NTP authentication is enabled, the switch will synchronize the time with NTP servers with trusted key only. For more information about trusted key, please see the ntp trustedkey command.
Examples

The following example shows how to enables NTP authentication:

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

Related Commands

```
show ntp
```

15.2.3 ntp broadcast client

Command Purpose

To configure the system to receive Network Time Protocol (NTP) broadcast packets on a specified interface, use the ntp broadcast client command in interface configuration mode. To disable this capability, use the no form of this command.

Command Syntax

```
ntp broadcast client
no ntp broadcast client
```

Command Mode

Interface Configuration

Default

NTP broadcast client is disabled by default

Usage

Use this command to allow the system to listen to broadcast packets on an interface-by-interface. Only physical interface, vlan interface and loopback interface support this command.

Examples

In the following example, the system is configured to receive (listen to) NTP broadcasts on Ethernet interface eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ntp broadcast client
```

Related Commands

```
ntp broadcastdelay
```

15.2.4 ntp broadcastdelay

Command Purpose

To configure the change the estimated round-trip delay between the switch and the NTP broadcast server, use the ntp broadcastdelay command in global configuration mode. To disable this capability, use the no form of this command.

Command Syntax

```
ntp broadcastdelay TIME
no ntp broadcastdelay
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIME</td>
<td>Delayed time interval in milliseconds, the range is 1-10000ms</td>
<td>1-10000 milliseconds</td>
</tr>
</tbody>
</table>

Command Mode

```
Global Configuration
```
Default
The default value should be 3000 milli-seconds.

Usage
None

Examples
The following example shows how to change broadcast delay to 2000ms:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config)# ntp broadcastdelay 2000

Related Commands
ntp broadcast client

15.2.5 ntp disable

Command Purpose
To configure Disable NTP packets from being received on the interface, use the ntp disable command in interface configuration mode. To disable this capability, use the no form of this command.

Command Syntax
ntp disable
no ntp disable

Command Mode
Interface Configuration

Default
By default, all interfaces receive NTP packets.

Usage
Only physical interface, vlan interface and loopback interface support this command.

Examples
In the following example, the system is configured not to receive NTP packet in interface eth-0-1:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config)# ntp disable

Related Commands
None

15.2.6 ntp key

Command Purpose
To configure value of the NTP key, use the ntp key command in global configuration mode. To remove the value of the NTP key, use the no form of this command.

Command Syntax
ntp key KEYID VALUE
no ntp key KEYID
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEYID</td>
<td>Authentication key</td>
<td>1-64000</td>
</tr>
<tr>
<td>VALUE</td>
<td>The value of the key</td>
<td>Up to 128 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

None

**Usage**

Use this command to create a value for a NTP key.

**Examples**

In the following example, the value 321 is given to the NTP key 123:

```
Switch# configure terminal
Switch(config)# ntp key 123 321
```

**Related Commands**

show ntp

---

**15.2.7 ntp interface reload**

**Command Purpose**

To reload the NTP configuration on the interfaces, use the ntp interface reload command in global configuration mode.

**Command Syntax**

```
ntp interface reload
```

**Command Mode**

Global Configuration

**Default**

None

**Usage**

Use this command to reload the NTP configuration on all the interfaces.

**Examples**

The following example reloads the NTP configuration on all interfaces:

```
Switch# configure terminal
Switch(config)# ntp interface reload
```

**Related Commands**

show ntp

---

**15.2.8 ntp max-distance**

**Command Purpose**

Use ntp max-distance command to config ntp max sync distance threshold. This command used in ntp client, and ntp calculate the sync distance to each ntp server and compare it with the ntp max sync distance which configured by ntp max-distance command. If the distance calculate by ntp over the distance configured by ntp max-distance, client will not sync with this ntp server.

**Command Syntax**

---
ntp max-distance DISTANCE
no ntp max-distance DISTANCE

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISTANCE</td>
<td>Specify the ntp max sync distance threshold in seconds, default 10s.</td>
<td>1-16</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

10

**Usage**

None

**Examples**

The following example shows the configuration of NTP:

```
Switch# configure terminal
DUT1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DUT1(config)# ntp max-distance 16
```

**Related Commands**

None

**15.2.9 ntp peer**

**Command Purpose**

To configure the software clock to synchronize a peer or to be synchronized by a peer, use the ntp peer command in global configuration mode. To disable this capability, use the no form of this command.

**Command Syntax**

```
ntp peer (HOSTNAME | IP_ADDR) { key KEY_ID | prefer | version VER } { source-interface IFNAME | source-ip SRC_ADDR }
no ntp peer (HOSTNAME | IP_ADDR)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOSTNAME</td>
<td>Name of the time server or peer</td>
<td>Up to 256 characters</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>IP address of the time server or peer</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>KEY_ID</td>
<td>Authentication key to use when sending packets to this peer</td>
<td>1-64000</td>
</tr>
<tr>
<td>prefer</td>
<td>Makes this peer the preferred peer that provides synchronization</td>
<td>-</td>
</tr>
<tr>
<td>VER</td>
<td>Defines the Network Time Protocol (NTP) version number</td>
<td>1-3</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Name of source interface</td>
<td>Support physical/aggregation/loopback/tunnel/vlan ports</td>
</tr>
<tr>
<td>SRC_ADDR</td>
<td>Source IP address</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration
Default
None

Usage
When a peer is configured, the default NTP version number is 3, no authentication key is used, and the source IP address is taken from the outgoing interface.
Use this command to allow a device to synchronize with a peer, or vice versa. Using the prefer keyword reduces switching between peers.
If the source interface or source IP address is specified, the packet transmit will use the related IP address as source address.
Examples
The following example shows how to configure a switch to allow its software clock to be synchronized with the clock of the peer (or vice versa) at IP address 192.168.22.33 using NTP version 2:
$Switch# configure terminal
Switch(config)# ntp peer 192.168.22.33 version 2

Related Commands
show ntp

15.2.10 ntp refclock

Command Purpose
To configure an external clock source for use with Network Time Protocol (NTP) services, use the ntp refclock command in global configuration mode. To disable support of the external time source, use the no form of this command.

Command Syntax
ntp refclock stratum NUMBER
no ntp refclock

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>Indicates the NTP stratum number that the system will claim.</td>
<td>1-15</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
This command is disabled by default.

Usage
None

Examples
The following example shows configuration of a NTP source on a switch platform:
$Switch# configure terminal
Switch(config)# ntp refclock stratum 1

Related Commands
show ntp

15.2.11 ntp server

Command Purpose
To allow the software clock to be synchronized by a Network Time Protocol (NTP) time server, use the ntp server command in global configuration mode. To disable this capability, use the no form of this command.

Command Syntax
ntp server (HOSTNAME | IP_ADDR) {key KEY_ID | prefer | version VER} {source-interface IFNAME | source-ip SRC_ADDR}
no ntp server (HOSTNAME | SRC_ADDR)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOSTNAME</td>
<td>Name of the time server or peer</td>
<td>Up to 256 characters</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>IP address of the time server or peer</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>KEY_ID</td>
<td>Authentication key to use when sending packets to this peer</td>
<td>1-64000</td>
</tr>
<tr>
<td>prefer</td>
<td>Makes this peer the preferred peer that provides synchronization</td>
<td>-</td>
</tr>
<tr>
<td>VER</td>
<td>Defines the Network Time Protocol (NTP) version number</td>
<td>1-3</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Name of source interface</td>
<td>Support physical/aggregation/loopback/tunnel/vlan ports</td>
</tr>
<tr>
<td>SRC_ADDR</td>
<td>Source IP address</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

The server will not synchronize to this machine.

**Usage**

Use this command if you want to allow the system to synchronize with the specified server.

If the source interface or source IP address is specified, the packet transmit will use the related IP address as source address.

**Examples**

The following example shows how to configure a switch to allow its software clock to be synchronized with the clock by the device at IP address 172.16.22.44 using NTP version 2:

```
Switch# configure terminal
Switch(config)# ntp server 172.16.22.44 version 2
```

**Related Commands**

`show ntp`

15.2.12 **ntp trustedkey**

**Command Purpose**

To authenticate the identity of a system to which Network Time Protocol (NTP) will synchronize, use the ntp trustedkey command in global configuration mode. To disable authentication of the identity of the system, use the no form of this command.

**Command Syntax**

```
ntp trustedkey KEY_ID
no ntp trustedkey KEY_ID
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEY_ID</td>
<td>Authentication key to use when sending packets to this peer</td>
<td>1-64000</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

None
Usage

If authentication is enabled, use this command to define one or more key numbers (corresponding to the keys defined with the ntp key command) that a peer NTP system must provide in its NTP packets, in order for this system to synchronize to it. This function provides protection against accidentally synchronizing the system to a system that is not trusted, because the other system must know the correct authentication key.

Examples

The following example shows how to configure the system to synchronize only to systems providing authentication key 42 in its NTP packets:

```
Switch# configure terminal
Switch(config)# ntp authentication enable
Switch(config)# ntp key 42 aNiceKey
Switch(config)# ntp trustedkey 42
```

Related Commands

- show ntp
- ntp key

15.2.13 show ntp

Command Purpose

To display the NTP configurations, use the ntp command in privileged EXEC mode.

Command Syntax

```
show ntp
```

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to display the NTP configurations.

Examples

The following example shows the configuration of NTP:

```
Switch# show ntp
Current NTP configuration:
=================================================================
NTP access control list:
Unicast peer:
  1.1.1.1
Unicast server:
  2.2.2.2
Broadcast client: enabled
Authentication: enabled
Local reference clock:
  enabled, stratum 10
```

Related Commands

- ntp server
- ntp peer

15.2.14 show ntp ace

Command Purpose

To display the restrict list of Access Control Entries (ACE) of a NTP server/peer, use the show ntp ace command in privileged EXEC mode.
Command Syntax

show ntp ace

Command Mode

Privileged EXEC

Default

None

Usage

None.

Examples

The following example shows the NTP restrict list:

Switch# show ntp ace

<table>
<thead>
<tr>
<th>address</th>
<th>mask</th>
<th>count</th>
<th>flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>55188</td>
<td>noquery, nomodify, notrap</td>
</tr>
<tr>
<td>6.6.6.6</td>
<td>255.255.255.255</td>
<td>73</td>
<td>none</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>255.255.255.255</td>
<td>1259</td>
<td>none</td>
</tr>
</tbody>
</table>

Related Commands

ntp ace

15.2.15 show ntp associations

Command Purpose

To show the status of Network Time Protocol (NTP) associations, use the show ntp associations command in privileged EXEC mode.

Command Syntax

show ntp associations

Command Mode

Privileged EXEC

Default

None

Usage

Detailed descriptions of the information displayed by this command can be found in the NTP specification (RFC 1305).

Examples

The following example shows the status of NTP associations:

Switch# show ntp associations

<table>
<thead>
<tr>
<th>remote</th>
<th>refid</th>
<th>st when poll reach</th>
<th>delay</th>
<th>offset</th>
<th>disp</th>
</tr>
</thead>
<tbody>
<tr>
<td>*6.6.6.6</td>
<td>127.127.1.0</td>
<td>6</td>
<td>161</td>
<td>256</td>
<td>377</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.778</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-0.087</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>119.400</td>
</tr>
</tbody>
</table>

* synchronized, + candidate, # selected, x falsetick, . excess, - outlyer

Related Commands

show ntp status
15.2.16 show ntp key

Command Purpose
To show the NTP keys, use the show ntp key command in privileged EXEC mode.

Command Syntax
show ntp key

Command Mode
Privileged EXEC

Default
None

Usage
Use this command to display the NTP keys.

Examples
The following example shows the keys of NTP:
Switch# show ntp key

Current NTP key configuration:
Flags: * - Trusted
ID | Value
--- | ---
* 1 | trusted_key
  5 | test_key

Related Commands
ntp key

15.2.17 show ntp status

Command Purpose
To show the status of the Network Time Protocol (NTP), use the show ntp status command in privileged EXEC mode.

Command Syntax
show ntp status

Command Mode
Privileged EXEC

Default
None

Usage
None.

Examples
The following is sample output from the show ntp status command:
Switch# show ntp status

Current NTP status:
#==================================================================
clock is synchronized
stratum: 11
reference clock: 127.127.1.0

http://www.fs.com
frequency: 0.000 ppm
precision: 2^15
reference time: d116c946.4dc2f6a7 (1:24:22.303 UTC Tue Mar 1 2011)
root delay: 0.000 ms
root dispersion: 449.207 ms
peer dispersion: 662.059 ms
clock offset: 0.000 ms
stability: 0.000 ppm

Related Commands

show ntp associations

15.2.18 show ntp statistics

Command Purpose
To show the statistics of the Network Time Protocol (NTP), use the show ntp statistics command in privileged EXEC mode.

Command Syntax
show ntp statistics

Command Mode
Privileged EXEC

Default
None

Usage
None.

Examples
The following is sample output from the show ntp statistics command:
Switch# show ntp statistics
Current NTP I/O statistics:
====================================================================
time since reset: 175834
receive buffers: 10
free receive buffers: 9
used receive buffers: 0
low water refills: 1
dropped packets: 0
ignored packets: 0
received packets: 32
packets sent: 31
packets not sent: 0
interrupts handled: 32
received by int: 32

Related Commands

show ntp associations

15.2.19 clear ntp statistics

Command Purpose
To clear the statistics of the Network Time Protocol (NTP), use the clear ntp statistics command in privileged EXEC mode.

Command Syntax
clear ntp statistics

Command Mode
Privileged EXEC
Privileged EXEC

Default

None

Usage

None.

Examples

The following is a sample to clear ntp statistics:
Switch# clear ntp statistics

Related Commands

show ntp statistics

15.2.20 ntp mgmt-if

Command Purpose

To enable NTP management interface, use the ntp mgmt-if command. To enable management interface only, use the only parameter. To enable both in-band and management interface, use the enable parameter. To disable NTP management interface, use the no ntp mgmt-if command.

Command Syntax

ntp mgmt-if ( enable | only )
no ntp mgmt-if

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>only</td>
<td>Only use management interface</td>
<td>-</td>
</tr>
<tr>
<td>enable</td>
<td>Both use management interface and in-band interface</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

Disable management interface by default and only use in-band interface

Usage

Use this command to enable management interface, then the ntp client will connect to the server or peer.

Examples

The following example shows only use management interface:
Switch# configure terminal
Switch(config)# ntp mgmt-if only

Related Commands

show ntp
ntp mgmt-if broadcast

15.2.21 ntp mgmt-if broadcast client

Command Purpose

To allow the system to listen to broadcast packets on management, use the ntp mgmt-if broadcast client command. To disable this capability, use the no form of this command.
Command Syntax

ntp mgmt-if broadcast client
no ntp mgmt-if broadcast client

Command Mode

Global Configuration

Default

NTP broadcast client is disabled by default

Usage

Use this command to allow the system to listen to broadcast packets on management interface.

Examples

In the following example, the system is configured to receive (listen to) NTP broadcasts on management interface:

Switch# configure terminal
Switch(config)# ntp mgmt-if broadcast client

Related Commands

show ntp
ntp mgmt-if

15.3 Phy Loopback Commands

15.3.1 loopback phy

Command Purpose

Use this command to configure a physical interface as phy level loopback mode. Use the no loopback command to cancel this configuration.

Command Syntax

loopback phy ( internal IFPHYSICAL | external )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal IFPHYSICAL</td>
<td>Packets transmitted to the interface should be looped back to a specified physical interface without any modification. The destination physical interface</td>
<td>-</td>
</tr>
<tr>
<td>external</td>
<td>Packets received from the interface should be looped back to the interface itself without any modification</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

None

Usage

Only one type of loopback can be applied on a physical interface. A new configuration should replace the old configuration.
Examples
In the following example, the physical interface is set to phy level loopback mode:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# loopback phy internal eth-0-2

Related Commands
no loopback

15.3.2 loopback port

Command Purpose
Use this command to configure a physical interface as port level loopback mode. Use the no loopback command to cancel this configuration.

Command Syntax
loopback port (mac-address swap | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-address swap</td>
<td>If this field is entered, the packet's SMAC incoming from port level loopback interface will be swapped with its DMAC, and the FCS will be updated</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
None

Usage
Only one type of loopback can be applied on a physical interface. A new configuration should replace the old configuration.

Examples
In the following example, the physical interface is set to port level loopback mode:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# loopback port

Related Commands
no loopback

15.3.3 no loopback

Command Purpose
Use this command to cancel a physical interface from phy level or port level loopback to normal interface.

Command Syntax
no loopback

Command Mode
Interface Configuration

Default
None
Usage

Phy or port level loopback can be canceled by this command.

Examples

In the following example, port level loopback is canceled by this command:

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

Related Commands

loopback phy
loopback port

15.3.4 show phy loopback

Command Purpose

Use this command to show the configuration of phy loopback.

Command Syntax

```
show phy loopback
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

In the following example shows how to show the configuration:

```
Switch# show phy loopback

Interface   Type   DestIntf   SwapMac
-----------  ------  ---------  ---
eth-0-1     port   -         no
eth-0-2     port   -         yes
eth-0-3     external -         -
eth-0-4     internal eth-0-5 -
```

Related Commands

loopback phy
loopback port

15.3.5 l2 ping

Command Purpose

Use this command to ping specified DMAC from specified physical interface, using protocol packet with ethertype 0x9009.

Command Syntax

```
l2 ping HHHH.HHHH.HHHH interface IFPHYSICAL ( ( vlan VLAN_ID | interval INTERVAL | timeout TIMEOUT | count COUNT | size SIZE ) )
```
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HHHH.HHHH.HHHH</td>
<td>The DMAC to ping</td>
<td>MAC Address in HHHH.HHHH.HHHH format</td>
</tr>
<tr>
<td>interface IFPHYSICAL</td>
<td>The interface to ping from</td>
<td>Support physical ports</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The vlan id of the protocol ping packet</td>
<td>1-4094</td>
</tr>
<tr>
<td>INTERVAL</td>
<td>The interval time between two ping action, second</td>
<td>1-65535</td>
</tr>
<tr>
<td>TIMEOUT</td>
<td>The time wait for a ping action, second</td>
<td>1-65535</td>
</tr>
<tr>
<td>COUNT</td>
<td>Total ping times</td>
<td>1-65535</td>
</tr>
<tr>
<td>SIZE</td>
<td>The size of the protocol ping packet</td>
<td>64-1518</td>
</tr>
</tbody>
</table>

### 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

- **15.3.6 l2 ping response**

### Command Purpose

Use this command to enable l2 ping response globally. Use the no form of this command to disable it.

### Command Syntax

- l2 ping response
- no l2 ping response

### Command Mode

**Interface Configuration**

### Default

None

### Usage

If l2 ping response is not enabled, the l2 ping request packet should be dropped.

### Examples

In the following example shows how to enable l2 ping response on interface:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# l2 ping response enable

Related Commands
l2 ping
show l2ping response

15.3.7 show l2ping response

Command Purpose
Use this command to show the configuration of l2 ping.

Command Syntax
show l2ping response

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
In the following example shows how to use this command:
Switch# show l2 ping response

<table>
<thead>
<tr>
<th>Interface</th>
<th>L2pingResp</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth-0-7</td>
<td>Enable</td>
</tr>
<tr>
<td>eth-0-8</td>
<td>Enable</td>
</tr>
</tbody>
</table>

Related Commands
l2 ping response

15.3.8 show l2ping state

Command Purpose

Command Syntax
show l2ping state

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
In the following example shows the status of l2ping:
Switch# show l2ping response

L2 ping state.

<table>
<thead>
<tr>
<th>Total count</th>
<th>Interval</th>
<th>Timeout</th>
<th>VlanId</th>
<th>Packet size</th>
<th>Sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>1515010</td>
<td>10</td>
<td>1</td>
<td>100</td>
<td>100</td>
</tr>
</tbody>
</table>

10 packet(s) transmitted, 0 received, 100 % packet loss

Related Commands
None

15.3.9 l2 ping stop

Command Purpose
Command Syntax
l2 ping stop

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
In the following example shows how to stop L2 ping:
Switch# l2 ping stop

Related Commands
None

15.3.10 l2 ping forward enable

Command Purpose
Command Syntax
l2 ping forward enable
no l2 ping forward enable

Command Mode
Interface Configuration

Default
Enable

Usage
None

Examples
In the following example shows how to enable L2 ping forward on interface:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# l2 ping forward enable
Related Commands
None

15.3.11 debug l2ping

Command Purpose
Use this command to enable debugging l2 ping.

Command Syntax
debug l2ping ( all | packet | send | receive | response )
no debug l2ping ( all | packet | send | receive | response )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>All l2ping debug</td>
<td>-</td>
</tr>
<tr>
<td>packet</td>
<td>Packet</td>
<td>-</td>
</tr>
<tr>
<td>send</td>
<td>Send packets</td>
<td>-</td>
</tr>
<tr>
<td>receive</td>
<td>Receive packets</td>
<td>-</td>
</tr>
<tr>
<td>response</td>
<td>Response Log</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
All these three debugging types is off.

Usage
If packet, send, or receive debugging is on, the corresponding message will be printed.

Examples
In the following example shows how to use this command:
Switch# debug l2ping all

Related Commands
l2 ping response

15.3.12 show debugging l2ping

Command Purpose
Use this command to show the status of l2ping debugging

Command Syntax
show debugging l2ping

Command Mode
Privileged EXEC

Default
None
Usage

None

Examples

In the following example shows the status of l2ping debugging:
Switch# show debugging l2ping

L2ping debugging status:
  l2ping packet debugging is on
  l2ping receive debugging is on
  l2ping send debugging is on
  l2ping response debugging is on

Related Commands

l2ping response

15.4 RMON Commands

15.4.1 rmon collection stats

Command Purpose

Use this command to enable RMON statistic collection on the interface

Command Syntax

rmon collection stats ID ( owner OWNER | )
no rmon collection stats ID

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Specify the RMON group of statistics</td>
<td>1-65535</td>
</tr>
<tr>
<td>owner OWNER</td>
<td>The owner identity of the statistic.(optional)</td>
<td>Up to 15 characters</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

None

Usage

To create one statistic only on a certain interface

Examples

This example shows how to collect RMON statistics for the owner test:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# rmon collection stats 1 owner test

Related Commands

show rmon statistics

15.4.2 rmon collection history

Command Purpose

Use this command to enable RMON history collection for the specified number of buckets and time period
Command Syntax
rmon collection history INDEX ( buckets NUMBER | ) ( interval INTERVAL | ) ( owner OWNER | )
no rmon collection history INDEX

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INDEX</td>
<td>Specify the maximum number of buckets desired for the RMON Collection history group of statistics.</td>
<td>1-65535</td>
</tr>
<tr>
<td>buckets NUMBER</td>
<td>Specify the maximum number of buckets desired for the RMON Collection history group of statistics.</td>
<td>1-65535</td>
</tr>
<tr>
<td>interval INTERVAL</td>
<td>Specify the number of seconds in each polling cycle.</td>
<td>1-3600</td>
</tr>
<tr>
<td>owner OWNER</td>
<td>The owner identity of history group (optional)</td>
<td>Up to 15 characters</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
None

Usage
Use this command to enable a history statistics on a certain interface.

Examples
This example shows how to enable history RMON statistics on eth-0-1:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# rmon collection history 1 buckets 1000 interval 100 owner test

Related Commands
show rmon history

15.4.3 rmon event

Command Purpose
Use this command to add an event to RMON event table

Command Syntax
rmon event INDEX ( log | ) ( trap TRAP | ) ( description DESCRIPTION | ) ( owner OWNER | )
no rmon event Index

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INDEX</td>
<td>Event index.</td>
<td>1-65535</td>
</tr>
<tr>
<td>log</td>
<td>Generate a RMON log when event is triggered</td>
<td>-</td>
</tr>
<tr>
<td>trap TRAP</td>
<td>Trap community</td>
<td>Up to 127 characters</td>
</tr>
<tr>
<td>description DESCRIPTION</td>
<td>Specify the description string for the event (default is RMON_SNMP)</td>
<td>Up to 127 characters</td>
</tr>
<tr>
<td>owner OWNER</td>
<td>The owner name (default is RMON_SNMP)</td>
<td>Up to 15 characters</td>
</tr>
</tbody>
</table>
Command Mode
Global Configuration

Default
None

Usage
Create an event is for RMON alarm. Permit event special triggered operate. Log can be sent by trap.

Examples
This example shows how to create an event:
Switch# configure terminal
Switch(config)# rmon event 1 log trap public description reach_max owner test

Related Commands
show rmon event

15.4.4 rmon alarm

Command Purpose
Use this command to set an alarm on a MIB object.

Command Syntax
rmon alarm INDEX OID interval INTERVAL (delta | absolute) rising-threshold RTHRE (event numbs | ) falling-threshold FTHRE (event NUMBER | ) (owner OWNER | )
no rmon alarm Index

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INDEX</td>
<td>Alarm index.</td>
<td>1-65535</td>
</tr>
<tr>
<td>OID</td>
<td>Variable for setting alarm(etherStatsEntry.m.n)</td>
<td>MIB OID</td>
</tr>
<tr>
<td>INTERVAL</td>
<td>Specify the time in seconds the alarm monitors the MIB object(seconds).</td>
<td>1-65535</td>
</tr>
<tr>
<td>delta</td>
<td>Specify the delta keyword to test the change between samples of a MIB variable</td>
<td>-</td>
</tr>
<tr>
<td>absolute</td>
<td>Specify the absolute keyword to test each MIB variable directly</td>
<td>-</td>
</tr>
<tr>
<td>rising-threshold RTHRE</td>
<td>Alarm rising threshold.</td>
<td>-2147483648 - 2147483646</td>
</tr>
<tr>
<td>event numbs</td>
<td>Specify the event number to trigger when the falling threshold</td>
<td>1-65535</td>
</tr>
<tr>
<td>falling-threshold FTHRE</td>
<td>Alarm falling threshold.</td>
<td>-2147483648-2147483646</td>
</tr>
<tr>
<td>event NUMBER</td>
<td>Specify the event number to trigger when the falling threshold</td>
<td>1-65535</td>
</tr>
<tr>
<td>owner OWNER</td>
<td>exceeds its limit.</td>
<td>Up to 15 characters</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None
Usage
We need to create events for rising threshold and falling threshold first before we create an alarm for a mib. Also the statistics need to be created on an interface, because we only support to set alarm monitor on etherStatsEntry.

Examples
This example shows how to set an alarm:
```
Switch# configure terminal
Switch(config)# rmon alarm 1 etherStatsEntry.3.1 interval 10 delta rising-threshold 1000 event 1 falling-threshold 5 event 1 owner test
```

Related Commands
None

15.4.5 show rmon statistics

Command Purpose
Use this command to show rmon statistics.

Command Syntax
```
show rmon statistics (ID |)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Statistics index</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
Show the interface statistics which collect by RMON

Examples
This example shows how to show rmon statistics:
```
Switch# show rmon statistics
```

```
Rmon collection index 1
  Statistics ifIndex = 1, Owner: RMON_SNMP
  Input packets 0, octets 0, dropped 0
  Broadcast packets 0, multicast packets 0, CRC alignment errors 0, collisions 0
  Undersized packets 0, oversized packets 0, fragments 0, jabbers 0
  # of packets received of length (in octets):
    64:0, 65-127:0, 128-255:0
    256-511:0, 512-1023:0, 1024-max:0
```

Related Commands
None

15.4.6 show rmon history

Command Purpose
Use this command to show rmon history statistics.

Command Syntax
```
show rmon history (ID |)
```

---

www.fs.com 1415
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>History index</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
Show the interface history statistics which collect by RMON

**Examples**
This example shows how to show rmon history statistics:
Switch# show rmon history

```
History index = 1
  Data source ifindex = 1
  Buckets requested = 1000
  Buckets granted = 1000
  Interval = 100
  Owner: test
  Sample # 1 Begin at 00:30:07
  Received 00 octets, 00 packets
  00 broadcast and 00 multicast packets
  00 undersized and 00 oversized packets
  00 fragments and 00 jabbers
  00 CRC alignment errors and 00 collisions.
  # of dropped packet events is 00
  Network utilization is estimated at 0
  Sample # 2 Begin at 00:31:47
  Received 00 octets, 00 packets
  00 broadcast and 00 multicast packets
  00 undersized and 00 oversized packets
  00 fragments and 00 jabbers
  00 CRC alignment errors and 00 collisions.
  # of dropped packet events is 00
  Network utilization is estimated at 0
  Sample # 3 Begin at 00:33:27
  Received 00 octets, 00 packets
  00 broadcast and 00 multicast packets
  00 undersized and 00 oversized packets
  00 fragments and 00 jabbers
  00 CRC alignment errors and 00 collisions.
  # of dropped packet events is 00
  Network utilization is estimated at 0
```

**Related Commands**
None

**15.4.7 show rmon event**

**Command Purpose**
Use this command to show rmon event.

**Command Syntax**

```
show rmon event (ID | )
```
**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
Show rmon events information

**Examples**
This example shows how to show rmon event:
```
Switch# show rmon event
```
```
event Index = 1
Description: RMON_SNMP
Event type Log & Trap
Event community name public
Last Time Sent = 00:00:00
Owner test
```

**Related Commands**
None

**15.4.8 show rmon alarm**

**Command Purpose**
Use this command to show rmon alarm

**Command Syntax**
```
show rmon alarm (ID | )
```

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
Show rmon alarm information

**Examples**
This example shows how to show rmon alarm:
```
Switch# show rmon alarm
```
```
alarm Index = 1
alarm status = VALID
alarm Interval = 3600
alarm Type is Delta
```
alarm Value = 00
alarm Rising Threshold = 100
alarm Rising Event = 1
alarm Falling Threshold = 10
alarm Falling Event = 1
alarm Owner is test

Related Commands
None

15.4.9 rmon clear counters

Command Purpose
Use this command to clear rmon counters.

Command Syntax
Command Mode
Interface Configuration

Default
None

Usage
Clear counters on a interface

Examples
This example shows how to clear rmon counters:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# rmon clear counters

Related Commands
None

15.4.10 debug rmon

Command Purpose
Use this command to open rmon debug.

Command Syntax
d debug rmon
no rmon debug

Command Mode
Privileged EXEC

Default
None

Usage
Open rmon debug

Examples
This example shows how to open rmon debug:
Switch# debug rmon

Related Commands
None
15.5 SNMP Commands

15.5.1 snmp-server access

Command Purpose
To set the access security of MIB view, use the snmp-server access command in global configuration mode. To remove the access security of MIB view, use the no form of this command.

Command Syntax
snmp-server access GROUP_NAME security-model usm (noauth | auth | priv) ( (read READ | write WRITE | notify NOTIFY) context CONTEXT (prefix | exact | ))
no snmp-server access GROUP_NAME security-model usm (noauth | auth | priv) (context CONTEXT)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_NAME</td>
<td>Name of the group</td>
<td>Up to 31 characters</td>
</tr>
<tr>
<td>security-model</td>
<td>Define the security model of the group</td>
<td>-</td>
</tr>
<tr>
<td>usm</td>
<td>SNMPv3 usm security model</td>
<td>-</td>
</tr>
<tr>
<td>auth</td>
<td>Specifies authentication of a packet without encrypting it</td>
<td>-</td>
</tr>
<tr>
<td>noauth</td>
<td>Specifies no authentication of a packet</td>
<td>-</td>
</tr>
<tr>
<td>priv</td>
<td>Specifies authentication of a packet with encryption</td>
<td>-</td>
</tr>
<tr>
<td>context CONTEXT</td>
<td>(Optional) Specifies the SNMP context to associate with this SNMP group and its views.</td>
<td>Up to 31 characters</td>
</tr>
<tr>
<td>prefix</td>
<td>The context only match the prefix</td>
<td>-</td>
</tr>
<tr>
<td>exact</td>
<td>The context should match the whole part</td>
<td>-</td>
</tr>
<tr>
<td>READ</td>
<td>(Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent</td>
<td>Up to 31 characters</td>
</tr>
<tr>
<td>WRITE</td>
<td>(Optional) Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.</td>
<td>Up to 31 characters</td>
</tr>
<tr>
<td>NOTIFY</td>
<td>(Optional) Specifies a notify view for the SNMP group. This view enables you to specify a notify, inform, or trap</td>
<td>Up to 31 characters</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
No SNMP access group is defined

Usage
The command is used to create a access security for MIB view.

Examples
The following is sample output from the snmp-server access command:
Switch# configure terminal
Switch(config)# snmp-server access manage security-model usm auth write _all_ read _all_

Related Commands

show snmp-server access

15.5.2 snmp-server community

Command Purpose

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP), use the snmp-server community command in global configuration mode. To remove the specified community string, use the no form of this command.

Command Syntax

snmp-server community STRING ( read-only | read-write ) ( view NAME )
no snmp-server community STRING

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>STRING</td>
<td>Community string that consists of 1 to 256 alphanumeric characters and functions much like a password, permitting access to SNMP. Blank spaces are not permitted in the community string</td>
<td>A string with 1-256 characters</td>
</tr>
<tr>
<td>read-only</td>
<td>Specifies read-only access. Authorized management stations can retrieve only MIB objects</td>
<td>-</td>
</tr>
<tr>
<td>read-write</td>
<td>Specifies read-write access. Authorized management stations can both retrieve and modify MIB objects</td>
<td>-</td>
</tr>
<tr>
<td>view NAME</td>
<td>Specifies a previously defined view. The view defines the objects available to the SNMP community</td>
<td>Up to 31 characters</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

No SNMP community string is defined

Usage

The no snmp-server command disables all versions of SNMP (SNMPv1, SNMPv2C, SNMPv3).

Examples

The following example shows how to set the read/write community string to newstring.: Switch# configure terminal Switch(config)# snmp-server community newstring read-write

Related Commands

snmp-server enable

15.5.3 snmp-server context

Command Purpose

To create a Simple Network Management Protocol (SNMP) context, use the snmp-server context command in global configuration mode. To delete an SNMP context, use the no form of this command.

Command Syntax

snmp-server context CONTEXT
no snmp-server context CONTEXT
**Parameter** | **Parameter Description** | **Parameter Value**
--- | --- | ---
CONTEXT | Name of the SNMP context being created | Up to 31 characters

**Command Mode**
Global Configuration

**Default**
No SNMP contexts are configured

**Usage**
When you use the no snmp-server context command, all SNMP instances in that context are deleted.

**Examples**
The following is sample output from the snmp-server context command:
```
Switch# configure terminal
Switch(config)# snmp-server context contextA
```

**Related Commands**
show snmp-server context

15.5.4 snmp-server enable

**Command Purpose**
To enable the SNMP function, use the snmp-server enable command in global configuration mode. To disable the SNMP function, use the no form of this command.

**Command Syntax**
```
snmp-server enable
no snmp-server enable
```

**Command Mode**
Global Configuration

**Default**
SNMP function is disabled

**Usage**
The command is used to enable or disable snmp global.

**Examples**
The following is sample output from the snmp-server enable command:
```
Switch# configure terminal
Switch(config)# snmp-server enable
```

**Related Commands**
show snmp

15.5.5 snmp-server engineID

**Command Purpose**
To specify the Simple Network Management Protocol (SNMP) engine ID on the local device, use the snmp-server engineID command in global configuration mode. To remove the configured engine ID, use the no form of this command.
Command Syntax

```
snmp-server engineID STRING
no snmp-server engineID
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>STRING</td>
<td>A string identifies the engine ID</td>
<td>String of a maximum of 64 characters that identifies the engine ID</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

An SNMP engine ID is generated automatically but is not displayed or stored in the running configuration. You can display the default or configured engine ID by using the show snmp-server engineID command.

**Usage**

The SNMP engine ID is a unique string used to identify the device for administration purposes. You do not need to specify an engine ID for the device. For further details on the SNMP engine ID, see RFC 2571.

**Examples**

The following is sample output from the snmp-server engineID command:

```
Switch# configure terminal
Switch(config)# snmp-server engineID 30383038303830383038
```

**Related Commands**

- `show snmp-server engineID`

**15.5.6 snmp-server group**

**Command Purpose**

To configure a new Simple Network Management Protocol (SNMP) group, use the snmp-server group command in global configuration mode. To remove a specified SNMP group, use the no form of this command.

**Command Syntax**

```
snmp-server group GROUP_NAME user USER_NAME security-model usm
no snmp-server group GROUP_NAME user user-name security-model usm
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_NAME</td>
<td>Name of the group</td>
<td>Up to 31 characters</td>
</tr>
<tr>
<td>USER_NAME</td>
<td>Name of the user in that group</td>
<td>Up to 31 characters</td>
</tr>
<tr>
<td>security-model</td>
<td>Define the group security model</td>
<td>-</td>
</tr>
<tr>
<td>usm</td>
<td>SNMPv3 usm model</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

No SNMP server groups are configured.
Usage
This command is used to add a new SNMP server group.

Examples
The following is sample output from the snmp-server group command:
Switch# configure terminal
Switch(config)# snmp-server group SampleA user User1 security-model usm

Related Commands
show snmp-server group

15.5.7 snmp-server notify

Command Purpose
To set the notification of traps for Simple Network Management Protocol (SNMP), use the snmp-server notify command in global configuration mode. To restore to the default value, use the no form of this command.

Command Syntax
snmp-server notify notify-name tag tag-name (inform | trap |)
no snmp-server notify notify-name

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOTIFY_NAME</td>
<td>Name of the notification</td>
<td>Up to 31 characters</td>
</tr>
<tr>
<td>TAG_NAME</td>
<td>Name of the tag</td>
<td>Up to 32 characters</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>inform</td>
<td>Set notify type(default is trap) to INFOR</td>
<td>-</td>
</tr>
<tr>
<td>trap</td>
<td>Set notify type(default is trap) to TRAP</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
No SNMP notify names are configured

Usage
This command is used to send events with the notification type of error to the SNMP server.

Examples
The following is sample output from the snmp-server notify command:
Switch# configure terminal
Switch(config)# snmp-server notify note tag tt

Related Commands
show snmp-server notify

15.5.8 snmp-server system-contact

Command Purpose
To set the system contact (sysContact) string, use the snmp-server system-contact command in global configuration mode. To remove the system contact information, use the no form of this command.
Command Syntax

snmp-server system-contact TEXT
no snmp-server system-contact

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TEXT</td>
<td>String that describes the system contact information</td>
<td>Up to 255 characters</td>
</tr>
</tbody>
</table>

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

15.5.9 snmp-server system-location

Command Purpose

To set the system location string, use the snmp-server system-location command in global configuration mode. To remove the location string, use the no form of this command.

Command Syntax

snmp-server system-location TEXT
no snmp-server system-location

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TEXT</td>
<td>String that describes the system contact information</td>
<td>Up to 255 characters</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

No system location string is set

Usage

This command is used to set the system location of the SNMP agent so that these descriptions can be accessed through the configuration file.

Examples

The following is an example of a system location string:

Switch# configure terminal
Switch(config)# snmp-server system-location Sample Place
Related Commands

snmp-server system-contact

15.5.10 snmp-server target-address

Command Purpose

To specify the recipient of a Simple Network Management Protocol (SNMP) notification message, use the snmp-server trap target-address command in global configuration mode. To remove the specified host from the configuration, use the no form of this command.

Command Syntax

```
snmp-server target-address NAME param PARAM (IPV4_ADDR | IPV6_ADDR) (udpport UDP_PORT | timeout TIMEOUT | retries RETRY) | (taglist LINE |)
```

```
no snmp-server target-address WORD (mgmt-if |)
```

Parameter | Parameter Description | Parameter Value
--- | --- | ---
NAME | The name of the target address | Up to 31 characters
PARAM | Define a param name which help to find target params table | Up to 31 characters
mgmt-if | Management port | -
IPV4_ADDR | IPv4 address | IPv4 Address
IPV6_ADDR | IPv6 address | IPv6 Address
udpport port | (Optional) Specifies that SNMP notifications or informs are to be sent to an SNMP manager. The default port is 162 | 0-65535
timeout number | (Optional) The timeout value. The default value is 1500 millisecond | 0-65535 millisecond
retries number | (Optional) The retry time. The default value is 3 | 0-255
taglist LINE | (Optional) The name of the taglist (128 tags are supported), split by blank. Max length is 255 character | Up to 255 characters

Command Mode

Global Configuration

Default

No snmp server is configured.

Usage

This command is used to configure a remote manager's IP address.

This command is used for SNMP v3.

Examples

The following is sample output from the snmp-server target-address command:

```
Switch# configure terminal
Switch(config)# snmp-server target-address targ1 param parm1 10.0.0.2 taglist tmptag
```

Related Commands

show snmp-server target-address
15.5.11 **snmp-server 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/ipsia/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`

15.5.12 **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 delay, use the `no` form of this command.

**Command Syntax**

```
snmp-server trap delay (linkup | linkdown) TIMER
no snmp-server trap delay (linkup | linkdown)
```

**Parameter | Parameter Description | Parameter Value**
---|---|---
TIMER | The time to delay up/down. Unit: 100 millisecond | 1-100

**Command Mode**

Global Configuration

**Default**

No delay is enabled
Usage

The link down and up trap will send immediately while link state change. The command can configure a delay time for link status trap. The unit is 100ms.

Examples

The following is sample output from the snmp-server trap enable command:
Switch# configure terminal
Switch(config)# snmp-server trap delay linkup 10

Related Commands

snmp-server trap target-address

15.5.13 snmp-server trap target-address

Command Purpose

To configure a remote trap manager's IP address, use the snmp-server target-address command in global configuration mode. To remove the configuration, use the no form of this command.

Command Syntax

snmp-server trap target-address ( mgmt-if | vrf VRF_NAME | ) ( IPV4_ADDR | IPV6_ADDR ) community COMMUNITY ( udpport UDP_PORT | )
no snmp-server trap target-address ( mgmt-if | vrf VRF_NAME | ) ( IPV4_ADDR | IPV6_ADDR ) community COMMUNITY ( udpport UDP_PORT | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt-if</td>
<td>Management port</td>
<td>-</td>
</tr>
<tr>
<td>vrf VRF_NAME</td>
<td>VRF name</td>
<td>Up to 15 characters</td>
</tr>
<tr>
<td>IPV4_ADDR</td>
<td>IPv4 address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IPV6_ADDR</td>
<td>IPv6 address</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>COMMUNITY</td>
<td>Password-like community string sent with the notification operation</td>
<td>Up to 255 characters</td>
</tr>
<tr>
<td>(Optional)</td>
<td>Specifies that SNMP notifications or informs are to be sent to an SNMP manager. The default port is 162</td>
<td>1-65535</td>
</tr>
<tr>
<td>UDP_PORT</td>
<td>(Optional) Specifies that SNMP notifications or informs are to be sent to an SNMP manager. The default port is 162</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

The router does not send any trap messages.

Usage

This command is used to specify the server target address to which the trap is sent.

Examples

The following is sample output from the snmp-server trap target-address command:
Switch# configure terminal
Switch(config)# snmp-server trap target-address mgmt-if 192.168.1.100 community test udpport 6000

Related Commands

snmp-server trap enable
15.5.14 snmp-server inform target-address

Command Purpose
To specify the recipient of a Simple Network Management Protocol (SNMP) inform message, use the snmp-server inform target-address command in global configuration mode. To remove the specified host from the configuration, use the no form of this command.

Command Syntax
```
snmp-server inform target-address (mgmt-if | vrf VRF_NAME | IPV4_ADDR | IPV6_ADDR) community COMMUNITY (udpport UDP_PORT |)
no snmp-server inform target-address (mgmt-if | vrf VRF_NAME | IPV4_ADDR | IPV6_ADDR) community COMMUNITY (udpport UDP_PORT |)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt-if</td>
<td>Management port</td>
<td>-</td>
</tr>
<tr>
<td>vrf</td>
<td>VRF name</td>
<td>Up to 15 characters</td>
</tr>
<tr>
<td>IPV4_ADDR</td>
<td>IPv4 address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IPV6_ADDR</td>
<td>IPv6 address</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>COMMUNITY</td>
<td>Password-like community string sent with the notification operation</td>
<td>Up to 255 characters</td>
</tr>
<tr>
<td>UDP_PORT</td>
<td>(Optional) Specifies that SNMP notifications or informs are to be sent to an SNMP manager. The default port is 162</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
The router does not send any inform messages

Usage
This command is used to specify the server target address to which the inform is sent.

Examples
The following is sample output from the snmp-server inform target-address command:
```
Switch# configure terminal
Switch(config)# snmp-server inform target-address mgmt-if 192.168.1.100 community test udpport 6000
```

Related Commands
None

15.5.15 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
```
### Command Mode

**Global Configuration**

### Default

No SNMPv3 users are configured

### Usage

To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides.

### Examples

The following is sample output from the `snmp-server usm-user` command:

```
Switch# configure terminal
Switch(config)# snmp-server usm-user user1 authentication md5 mypassword privacy des yourpassword
```

### Related Commands

- `snmp-server engineID`

### 15.5.16  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
```
### Command Mode

Global Configuration

### Default

Support all SNMP versions

### Usage

This command is used to set the SNMP version the switch supported.

### Examples

The following is sample output from the snmp-server version command:

```
Switch# configure terminal
Switch(config)# snmp-server version all
```

### Related Commands

- show snmp-server version

### 15.5.17 snmp-server view

#### Command Purpose

To create or update a view entry, use the snmp-server view command in global configuration mode. To remove the specified Simple Network Management Protocol (SNMP) server view entry, use the no form of this command.

#### Command Syntax

```
snmp-server view NAME (included | excluded) sub-tree (mask MASK)
no snmp-server view NAME (included | excluded) sub-tree
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Label for the view record that you are updating or creating. The name is used to reference the record</td>
<td>Up to 31 characters</td>
</tr>
<tr>
<td>included</td>
<td>Configures the OID (and subtree OIDs) specified in sub-tree argument to be included in the SNMP view</td>
<td>-</td>
</tr>
<tr>
<td>excluded</td>
<td>Configures the OID (and subtree OIDs) specified in sub-tree argument to be explicitly excluded from the SNMP view</td>
<td>-</td>
</tr>
<tr>
<td>sub-tree</td>
<td>Object identifier of the ASN.1 subtree to be included or excluded from the view</td>
<td>-</td>
</tr>
<tr>
<td>MASK</td>
<td>Define the subtree mask</td>
<td>Up to 32 hexadecimal</td>
</tr>
</tbody>
</table>
Command Mode
Global Configuration

Default
No view entry exists

Usage
Other SNMP commands require an SMP view as an argument. You use this command to create a view to be used as arguments for other commands.

Examples
The following is sample output from the snmp-server view command:
Switch# configure terminal
Switch(config)# snmp-server view abc excluded 1.3.6.2

Related Commands
show snmp-server view

15.5.18  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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Access-list name</td>
<td>Up to 40 characters</td>
</tr>
<tr>
<td>in</td>
<td>Inbound packets</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
No access group is defined

Usage
The command is used to apply ACL in snmp.

Examples
The following is sample output from the snmp-server access command:
Switch# configure terminal
Switch(config)# snmp-server access-group abc in

Related Commands
None
15.5.19 show snmp

Command Purpose
To display the services information of SNMP, use the show snmp command in privileged EXEC mode.

Command Syntax
show snmp

Command Mode
Privileged EXEC

Default
None

Usage
This command is used to display the service information of SNMP (enable or disable).

Examples
The following is sample output from the show snmp command:
Switch# show snmp
SNMP services: enable

Related Commands
snmp-server enable

15.5.20 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 | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_NAME</td>
<td>Specify a group name</td>
<td>Up to 31 characters</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
This command is used to display the access information configured by command snmp-server access.

Examples
The following is sample output from the show snmp-server access command:
Switch# show snmp-server access gp1
Group name: gp1
Context: test
Security model: usm
Security level: auth
Context Match: exact
Read view: _all_
Write view: none
Notify view: none
Storage Type: permanent
Row status: active

Related Commands

snmp-server access

15.5.21 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

<table>
<thead>
<tr>
<th>Community-Access</th>
<th>Community-String</th>
<th>Security-name</th>
</tr>
</thead>
<tbody>
<tr>
<td>read-only</td>
<td>public</td>
<td>comm1</td>
</tr>
<tr>
<td>read-write</td>
<td>private</td>
<td>comm2</td>
</tr>
</tbody>
</table>

Related Commands

snmp-server community

15.5.22 show snmp-server context

Command Purpose
To display the SNMP context information, use the show snmp-server context command in privileged EXEC mode.

Command Syntax
show snmp-server context

Command Mode
Privileged EXEC

Default
None
Usage
This command is used to display the context information configured by command snmp-server context.

Examples
The following is sample output from the show snmp-server context command:
Switch# show snmp-server context
samplecontext

Related Commands
snmp-server context

15.5.23 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

15.5.24 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 | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_NAME</td>
<td>Specify a group name</td>
<td>Up to 31 characters</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Group-name</th>
<th>model</th>
<th>Security-name</th>
</tr>
</thead>
<tbody>
<tr>
<td>a11</td>
<td>usm</td>
<td>a</td>
</tr>
<tr>
<td>a11</td>
<td>usm</td>
<td>ab</td>
</tr>
</tbody>
</table>

Related Commands
snmp-server group

15.5.25 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 | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP_NAME</td>
<td>Specify a group name</td>
<td>Up to 31 characters</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Notify-name</th>
<th>Notify-type</th>
</tr>
</thead>
<tbody>
<tr>
<td>sample</td>
<td>trap</td>
</tr>
</tbody>
</table>

Related Commands
snmp-server notify
15.5.26 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: Denver
```

Related Commands
snmp-server system-contact
snmp-server system-location

15.5.27 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-addr.

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-address

15.5.28 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 | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>USERNAME</td>
<td>(Optional) Name of a specific user or users about which to display SNMP information</td>
<td>Up to 31 characters</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

An SNMP user must be part of an SNMP group, as configured using the snmp-server usm-user command.

Examples

The following is sample output from the show snmp-server usm-user command:

```
Switch# show snmp-server usm-user user1
EngineID: 01234567890123456789
User Name: user1
Auth Protocol: md5
priv Protocol: des
Storage Type: nonvolatile
Row status: active
```

Related Commands

snmp-server usm-user

15.5.29 show snmp-server version

Command Purpose

To display the supported version of SNMP, use the show snmp-server version command in privileged EXEC mode.

Command Syntax

show snmp-server version

Command Mode

Privileged EXEC

Default

None
Usage

This command is used to display snmp version information configured by command snmp-server version.

Examples

The following is sample output from the show snmp-server version command:

```
Switch# show snmp-server version
SNMPv1/SNMPv2c/SNMPv3
```

Related Commands

snmp-server version

15.5.30 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 [ ] )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Specify a view name</td>
<td>Up to 31 characters</td>
</tr>
</tbody>
</table>

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

snmp-server view
15.6 SFLOW Commands

15.6.1 sflow enable

Command Purpose
Use this command to enable or disable sFlow globally.

Command Syntax
sflow enable
no sflow enable

Command Mode
Global Configuration

Default
Disabled

Usage
Before any other sFlow command can be configured, sFlow services must be enabled globally. Use the no parameter with this command to remove all sFlow configurations and disable sFlow globally.

Examples
This example shows how to enable sFlow services globally:
Switch# configure terminal
Switch(config)# sflow enable

Related Commands
show sflow

15.6.2 sflow agent

Command Purpose
Use this command to configure sFlow agent.

Command Syntax
sflow agent ( ip IPV4_ADDR | ipv6 ipv6-address )
no sflow agent ( ip | ipv6 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPV4_ADDR</td>
<td>Agent IPv4 address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IPV6_ADDR</td>
<td>Agent IPv6 address</td>
<td>IPv6 Address</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
Use this command to configure IP address for sflow agent. If not configured and router-id has configured, sflow will use the valid interface with max router-id and then never change.
Examples

This example shows how to configure agent with IP address 10.0.0.254:
Switch# configure terminal
Switch(config)# sflow agent ip 10.0.0.254

Related Commands

show sflow

15.6.3 sflow collector

Command Purpose

Use this command to configure sFlow collector.

Command Syntax

sflow collector ( IPV4_ADDR | ipv6-address ) ( UDP_PORT | )
no sflow collector ( IPV4_ADDR | ipv6-address ) ( <UDP_PORT | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPV4_ADDR</td>
<td>Collector IPv4 address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IPV6_ADDR</td>
<td>Collector IPv6 address</td>
<td>IPv6 Address</td>
</tr>
<tr>
<td>UDP_PORT</td>
<td>Collector UDP port number, default is 6343</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

Use this command to add a collector by specifying the combination of IP address and UDP port. Only up to two unique combinations can be allowed to add. Use the no parameter with this command to delete collector.

Examples

This example shows how to add a collector with IP address 10.0.0.254 and UDP port 3000:
Switch# configure terminal
Switch(config)# sflow collector 10.0.0.254 3000

Related Commands

show sflow

15.6.4 sflow counter interval

Command Purpose

Use this command to configure sFlow polling-interval for counter sample.

Command Syntax

sflow counter interval INTERVAL
no sflow counter interval
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>Interval value in second</td>
<td>1-2000 second</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

20 seconds

**Usage**

Use this command to set sFlow polling-interval for counter sample. Use the no parameter with this command to restore to the default value. Default interval value is 20 seconds.

**Examples**

This example shows how to set sFlow polling-interval to 10 second:

Switch# configure terminal
Switch(config)# sflow counter-interval 10

**Related Commands**

show sflow

15.6.5 sflow counter-sampling enable

**Command Purpose**

Use this command to enable or disable counter sampling on specified port.

**Command Syntax**

```
sflow counter-sampling enable
no sflow counter-sampling enable
```

**Command Mode**

Interface Configuration

**Default**

Disabled

**Usage**

Use this command to enable counter sampling on specified port. Use the no parameter with this command to disable counter sampling. By default, sFlow counter sampling is disabled in all ports. This command can only be configured on a port which is not a link-agg group member. The port can be either a physical port or a link-agg port.

**Examples**

This example shows how to enable sFlow counter sampling on interface eth-0-1:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# sflow counter-sampling enable

**Related Commands**

show sflow
15.6.6 sflow flow-sampling rate

**Command Purpose**
Use this command to configure flow sampling rate.

**Command Syntax**
sflow flow-sampling rate RATE
no sflow flow-sampling rate

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RATE</td>
<td>Sample rate value</td>
<td>must be a power of 2, the range is 32-1048576</td>
</tr>
</tbody>
</table>

**Command Mode**
Interface Configuration

**Default**
8192

**Usage**
Use this command to set sFlow packet sampling rate. Use no parameter with this command to set default sampling rate. Default sampling rate value is 8192. sFlow uses CPU resources to collect samples and send samples to the collector. If a low sampling rate is set, CPU utilization can become high. To protect CPU from overwhelming, exceeded flow samples would be dropped. If a sampling rate less than default value is configured, a prompt will be given to info the potential of involving a high CPU utilization. This command can only be configured on a port which is not a link-agg group member. The port can be either a physical port or a link-agg port.

**Examples**
This example shows how to set the sFlow sampling rate to 2048 on eth-0-1:
```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# sflow flow-sampling rate 2048
```

Warning: sFlow sampling requires high CPU usage, especially with a low rate. It is suggested not configure a rate less than default value 8192.

**Related Commands**
show sflow

15.6.7 sflow flow-sampling enable

**Command Purpose**
Use this command to enable or disable packet sampling on individual port.

**Command Syntax**
sflow flow-sampling enable ( input | output | both )
no sflow flow-sampling enable ( input | output | both )

**Command Mode**
Interface Configuration

**Default**
Disabled
**Usage**

Use this command to enable ingress direction of packet sampling on individual port. Use the no parameter with this command to disable packet sampling. By default, sFlow packet sampling is disabled in all ports. This command can only be configured on a port which is not a link-agg group member. The port can be either a physical port or a link-agg port.

**Examples**

This example shows how to enable input packet sampling on route port eth-0-1:

```
Switch(config)# interface eth-0-1
Switch(config-if)# sflow flow-sampling enable input
```

**Related Commands**

show sflow

**15.6.8 show sflow**

**Command Purpose**

Use this command to show the running information of sflow.

**Command Syntax**

```
show sflow
```

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

Use this command to show the running information of sflow.

**Examples**

This example shows how to show the sflow running information:

```
Switch# show sflow
```

```
sFlow Version: 5
sFlow Global Information:
  Agent IP address: 0.0.0.0
  Collector IP: Not configured
  Counter Sampling Interval: 20 seconds
sFlow Port Information:
   Flow-Sample     Flow-Sample
   Counter Flow     Direction Rate
  eth-0-1 Disable Enable Input 8192
```

**Related Commands**

sflow enable
sflow collector
15.7 LLDP Commands

15.7.1 llpd enable(global)

Command Purpose
To enable LLDP function globally, use the llpd enable command in global configuration mode. To disable this function, use the no form of this command.

Command Syntax
llpd enable
llpd disable

Command Mode
Global Configuration

Default
Disable

Usage
None

Examples
The following example shows how to enable LLDP globally:
Switch# configure terminal
Switch(config)# llpd enable

Related Commands
llpd enable (interface)

15.7.2 llpd enable(interface)

Command Purpose
To enable LLDP function on interface, use the llpd enable command in interface configuration mode. To disable this function, use the no form of this command.

Command Syntax
llpd enable (txonly | txrx | rxonly )
llpd disable

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>txonly</td>
<td>Enable llpd pdu transmission</td>
<td>-</td>
</tr>
<tr>
<td>txrx</td>
<td>Enable llpd pdu transmission and reception</td>
<td>-</td>
</tr>
<tr>
<td>rxonly</td>
<td>Enable llpd pdu reception</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
Enable
Usage
None

Examples
The following example shows how to enable LLDP on interface:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# lldp enable txrx

Related Commands
lldp enable (global)

15.7.3 lldp system-name

Command Purpose
To configure system name for System Name TLV, use the lldp system-name command in global configuration mode. To restore the default configuration, use the no form of this command.

Command Syntax
lldp system-name NAME
go lldp system-name

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>System Name.</td>
<td>A string with 1-64 characters</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
Default system name is used.

Usage
If no system name is configured, the default system name will be used.

Examples
The following example shows how to configure system name:
Switch# configure terminal
Switch(config)# lldp system-name switch

Related Commands
lldp enable (global)
lldp enable (interface)

15.7.4 lldp system-description

Command Purpose
To configure system description for System Description TLV, use the lldp system-description command in global configuration mode. To restore the default configuration, use the no form of this command.

Command Syntax
lldp system-description LINE
go lldp system-description

www.fs.com
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LINE</td>
<td>System Description. The range is from 1 to 255 and space is allowed</td>
<td>A string with 1-255 characters</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
Default system description is used.

**Usage**
If no system description is configured, the default system description will be used.

**Examples**
The following example shows how to configure system description:
Switch# configure terminal
Switch(config)# lldp system-description switch

**Related Commands**
lldp enable (global)
lldp enable (interface)

## 15.7.5 lldp management

**Command Purpose**
To configure management ip address for Management Address TLV, use the lldp management ip command in global configuration mode. To restore the default configuration, use the no form of this command.

**Command Syntax**
```
lldp management (ip ADDRESS | interface IFNAME )
no lldp management ( ip | interface )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADDRESS</td>
<td>IPv4 address, like 1.1.1.1</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Name of L3 interface</td>
<td>Support physical/aggregation/loopback/vlan/tunnel/management ports</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
Default management address is used.

**Usage**
The configured IP address has higher priority than configured interface. If both of them are not be configured, system should use the loopback interface, 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
15.7.6  lldp msg-tx-hold

Command Purpose
To configure msg-tx-hold, use the lldp msg-tx-hold command in global configuration. To restore the default configuration, use the no form of this command.

Command Syntax
lldp msg-tx-hold NUMBER
no lldp msg-tx-hold

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>msg-tx-hold value</td>
<td>2-10</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
The default value of msg-tx-hold is 4.

Usage
None

Examples
The following example shows how to configure msg-tx-hold:
Switch# configure terminal
Switch(config)# lldp msg-tx-hold 3

Related Commands
lldp enable (global)
lldp enable (interface)

15.7.7  lldp timer msg-tx-interval

Command Purpose
To configure msg-tx-interval, use the lldp timer msg-tx-interval command in global configuration. To restore the default configuration, use the no form of this command.

Command Syntax
lldp timer msg-tx-interval NUMBER
no lldp timer msg-tx-interval

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>msg-tx-interval value</td>
<td>msg-tx-hold</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration
Default
The default value of msg-tx-interval is 30s.

Usage
None

Examples
The following example shows how to configure msg-tx-interval:
Switch# configure terminal
Switch(config)# lldp timer msg-tx-interval 20

Related Commands
lldp enable (global)
lldp enable (interface)

15.7.8 lldp timer reinit-delay

Command Purpose
To configure reinitDelay, use the lldp timer reinitDelay command in global configuration. To restore the default configuration, use the no form of this command.

Command Syntax
lldp timer reinit-delay NUMBER
no lldp timer reinit-delay

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>reinit-delay value</td>
<td>1-10</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
The default value of reinitDelay is 2s.

Usage
None

Examples
The following example shows how to configure reinitDelay:
Switch# configure terminal
Switch(config)# lldp timer reinit-delay 1

Related Commands
lldp enable (global)
lldp enable (interface)

15.7.9 lldp timer tx-delay

Command Purpose
To configure tx-delay, use the lldp timer tx-delay command in global configuration. To restore the default configuration, use the no form of this command.
Command Syntax

lldp timer tx-delay NUMBER
no lldp timer tx-delay

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER</td>
<td>tx-delay value</td>
<td>1-8192</td>
</tr>
</tbody>
</table>

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)

15.7.10  lldp tlv basic

Command Purpose

To select the basic tlv used in LLDP packet, use the lldp tlv basic command in interface configuration. To cancel the tlv, use the no form of this command.

Command Syntax

lldp tlv basic { port-description | system-name | system-description | system-capabilities | management-address | all }
no lldp tlv basic { port-description | system-name | system-description | system-capabilities | management-address | all }

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-description</td>
<td>Select Port Description Tlv</td>
<td>-</td>
</tr>
<tr>
<td>system-name</td>
<td>Select System Name Tlv</td>
<td>-</td>
</tr>
<tr>
<td>system-description</td>
<td>Select System Description Tlv</td>
<td>-</td>
</tr>
<tr>
<td>system-capabilities</td>
<td>Select System Capabilities Tlv</td>
<td>-</td>
</tr>
<tr>
<td>management-address</td>
<td>Select Management Address Tlv</td>
<td>-</td>
</tr>
<tr>
<td>all</td>
<td>Select All basic tlvs</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration
Default
All basic tlv is selected.

Usage
None

Examples
The following example shows how to select basic tlv:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# lldp tlv basic system-name

Related Commands
lldp enable (global)
lldp enable (interface)

15.7.11 lldp tlv 8021-org-specific

Command Purpose
To select the IEEE 802.1 tlv used in LLDP packet, use the lldp tlv 8021-org-specific command in interface configuration. To cancel the tlv, use the no form of this command.

Command Syntax
lldp tlv 8021-org-specific { port-vlan | protocol-vlan | vlan-name | protocol-id | link-aggregation | dcbx | all }
no lldp tlv 8021-org-specific { port-vlan | protocol-vlan | vlan-name | protocol-id | link-aggregation | dcbx | all }


<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-vlan</td>
<td>Select Port Vlan ID Tlv</td>
<td>-</td>
</tr>
<tr>
<td>protocol-vlan</td>
<td>Select Port and Protocol Vlan ID Tlv</td>
<td>-</td>
</tr>
<tr>
<td>vlan-name</td>
<td>Select Vlan Name Tlv</td>
<td>-</td>
</tr>
<tr>
<td>protocol-id</td>
<td>Select Protocol Identity Tlv</td>
<td>-</td>
</tr>
<tr>
<td>link-aggregation</td>
<td>Select Link Aggregation Tlv</td>
<td>-</td>
</tr>
<tr>
<td>dcbx</td>
<td>Select DCBX TLV</td>
<td>-</td>
</tr>
<tr>
<td>all</td>
<td>Select All IEEE 802.1 tlv, exclude Link Aggregation Tlv</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
All IEEE 802.1 tlv is selected, exclude Link Aggregation Tlv.

Usage
Link Aggregation Tlv in IEEE 802.3 tlv set is used by default.

Examples
The following example shows how to select IEEE 802.1 tlv:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# lldp tlv 8021-org-specific vlan-name
Related Commands
lldp enable(global)
lldp enable(interface)
lldp tlv 8021-org-specific vlan-name-value

Command Purpose
To configure the value for VLAN NAME TLV in the IEEE 802.1 tlv, use the lldp tlv 8021-org-specific vlan-name-value command in interface configuration. To cancel the configuration, use the no form of this command.

Command Syntax
lldp tlv 8021-org-specific vlan-name-value VLAN_ID
no lldp tlv 8021-org-specific vlan-name-value

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>The value of Vlan ID for the VLAN NAME TLV</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
The VLAN NAME TLV will contain the information of native vlan.

Usage
None

Examples
The following example shows how to configure VLAN NAME TLV:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# lldp tlv 8021-org-specific vlan-name-value 2000

Related Commands
lldp enable (global)
lldp enable (interface)

15.7.12 lldp tlv 8023-org-specific

Command Purpose
To select the IEEE 802.3 tlv used in LLDP packet, use the lldp tlv 8023-org-specific command in interface configuration. To cancel the tlv, use the no form of this command.

Command Syntax
lldp tlv 8023-org-specific { mac-phy-cfg | power | link-aggregation | max-frame-size | all }
no lldp tlv 8023-org-specific { mac-phy-cfg | power | link-aggregation | max-frame-size | all }

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-phy-cfg</td>
<td>Select MAC/PHY Configuration/Status TLV</td>
<td>-</td>
</tr>
<tr>
<td>power</td>
<td>Select Power Via MDI Tlv</td>
<td>-</td>
</tr>
<tr>
<td>link-aggregation</td>
<td>Select Link Aggregation Tlv</td>
<td>-</td>
</tr>
<tr>
<td>max-frame-size</td>
<td>Select Maximum Frame Size Tlv</td>
<td>-</td>
</tr>
<tr>
<td>all</td>
<td>Select All IEEE 802.3 tlv</td>
<td>-</td>
</tr>
</tbody>
</table>
**Command Mode**

Interface Configuration

**Default**

All IEEE 802.3 tlv is selected.

**Usage**

Link Aggregation Tlv in IEEE 802.3 tlv set is used by default.

**Examples**

The following example shows how to select IEEE 802.3 tlv:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# lldp tlv 8023-org-specific power
```

**Related Commands**

lldp enable(global)
lldp enable(interface)

15.7.13 lldp tlv med

**Command Purpose**

To select the MED tlv used in LLDP packet, use the lldp tlv med command in interface configuration. To cancel the tlv, use the no form of this command.

**Command Syntax**

```
lldp tlv med { network-policy | ext-power | inventory | all }
```

```
no lldp tlv med { network-policy | ext-power | inventory | all }
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>network-policy</td>
<td>Select Network Policy TLV</td>
<td>-</td>
</tr>
<tr>
<td>ext-power</td>
<td>Select Extend Power-Via-MDI TLV</td>
<td>-</td>
</tr>
<tr>
<td>inventory</td>
<td>Select Inventory TLv</td>
<td>-</td>
</tr>
<tr>
<td>all</td>
<td>Select All MED tlv, exclude Location Identification TLv</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

All MED tlv 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)

15.7.14 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ecs-elin VALUE</td>
<td>The ECS-ELIN address should be a telephone number</td>
<td>The ECS-ELIN address should be a telephone number in range [10-25]</td>
</tr>
<tr>
<td>civic DEV-TYPE</td>
<td>DEV-TYPE, 0 - DHCP Server, 1 - the closet network device, 2 - current devic</td>
<td>0-2</td>
</tr>
<tr>
<td>CODE</td>
<td>The two-letter ISO 3166 country code in capital ASCII letters, eg., US</td>
<td>CODE, The two-letter ISO 3166 country code in capital ASCII letters</td>
</tr>
<tr>
<td>CA(n)-TYPE CA(n)-VALUE</td>
<td>n = 1-10</td>
<td>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]</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
None

Usage
None

Examples
The following example shows how to configure MED location-id tlv:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# lldp tlv med location-id ecs-elin 1234567890

Related Commands
lldp enable (global)
lldp enable (interface)

15.7.15 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 }

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>events</td>
<td>LLDP events</td>
<td>-</td>
</tr>
<tr>
<td>packet</td>
<td>LLDP Packet information</td>
<td>-</td>
</tr>
<tr>
<td>all</td>
<td>Turn all debugging on</td>
<td>-</td>
</tr>
<tr>
<td>tlv-info</td>
<td>Enable TLV information debugs</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
Use command "terminal monitor" to make debug messages print on the VTY immediately. Use command "show logging buffer" to check the debug messages in the logging buffer.

**Examples**
The following is sample to open lldp debug switches:
```
Switch# debug lldp all
```

**Related Commands**
terminal monitor
show logging buffer

**15.7.16 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 | }
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>Configuration Information</td>
<td>-</td>
</tr>
<tr>
<td>tlv-info</td>
<td>Local LLDP TLV information</td>
<td>-</td>
</tr>
<tr>
<td>interface</td>
<td>Display LLDP configuration or tlv information of special interface</td>
<td>-</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Interface name, only allowed physical interface</td>
<td>Support physical ports</td>
</tr>
</tbody>
</table>

**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

15.7.17 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 | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Display LLDP neighbor information of special interface</td>
<td>-</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Interface name. only allowed physical interface</td>
<td>Support physical ports</td>
</tr>
<tr>
<td>brief</td>
<td>Display brief information</td>
<td>-</td>
</tr>
</tbody>
</table>
**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
```

<table>
<thead>
<tr>
<th>Local Port</th>
<th>eth-0-4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Port</td>
<td>eth-0-6</td>
</tr>
<tr>
<td>Hold Time</td>
<td>120</td>
</tr>
<tr>
<td>Expire Time</td>
<td>116</td>
</tr>
<tr>
<td>System Name</td>
<td>switch</td>
</tr>
</tbody>
</table>

**Related Commands**

- `lldp enable(global)`
- `lldp enable(interface)`

### 15.7.18 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Display LLDP statistics of special interface</td>
<td>-</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Interface name. only allowed physical interface</td>
<td>Support physical ports</td>
</tr>
</tbody>
</table>

**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 Received: 364
TLVs discarded: 0
TLVs unrecognized: 0

Related Commands

clear lldp statistics
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 | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Clear LLDP statistics of special interface</td>
<td>-</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Interface name, only allowed physical interface</td>
<td>Support physical ports</td>
</tr>
</tbody>
</table>

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

15.8 IPFIX Commands

15.8.1 ipfix recorder

Command Syntax

ipfix recorder NAME
no ipfix recorder NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>ipfix recorder name</td>
<td>Up to 32 characters</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None
Usage

If ipfix recorder has existed, it will enter IPFIX recorder Configuration; if ipfix recorder is new, it will create a recorder and enter IPFIX recorder Configuration; this command should work with the commands of match and collect.

Examples

This example shows how to create ipfix recorder recorder1 in global configuration and enter IPFIX recorder Configuration:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure terminal</td>
<td>Switch(config)# ipfix recorder recorder1</td>
</tr>
<tr>
<td>Switch(config)# ipfix recorder recorder1</td>
<td>Switch(Config-ipfix-reocrder)#</td>
</tr>
</tbody>
</table>

Delete ipfix recorder recorder1:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure terminal</td>
<td>Switch(config)# no ipfix recorder recorder1</td>
</tr>
<tr>
<td>Switch(config)# no ipfix recorder recorder1</td>
<td></td>
</tr>
</tbody>
</table>

Related Commands
description
match ipv4
match ipv6
match mpls
match transport
collect ttl
collect flow
collect counter

15.8.2 description

Command Purpose

This command used to describe ipfix recorder. use the no form of this command to delete this description.

Command Syntax
description DESCRIPTION

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DESCRIPTION</td>
<td>ipfix monitor description</td>
<td>The length of ipfix monitor description should not exceed 64 characters</td>
</tr>
</tbody>
</table>

Command Mode

IPFIX recorder Configuration

Default
None

Usage
None

Examples

This example shows how to describe recorder in IPFIX recorder Configuration:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure terminal</td>
<td>Switch(config)# ipfix recorder recorder1</td>
</tr>
<tr>
<td>Switch(config)# ipfix recorder recorder1</td>
<td>Switch(Config-ipfix-reocrder)# description this is a ipfix recorder</td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td>Switch(config)# ipfix recorder recorder1</td>
</tr>
<tr>
<td>Switch(config)# ipfix recorder recorder1</td>
<td>Switch(Config-ipfix-reocrder)# no description</td>
</tr>
</tbody>
</table>

Related Commands
None
15.8.3 match ipv4

Command Purpose
This command configures the fields of ipv4 in ipfix recorder, use the no form of this command to delete this configure.

Command Syntax
match ipv4 ( source | destination ) address ( mask IP_MASK_LEN )
match ipv4 ( dscp | ecn | ttl )
no match ipv4 ( source | destination ) address
no match ipv4 ( dscp | ecn | ttl )

Parameter | Parameter Description | Parameter Value
--- | --- | ---
source | ipv4 source ipaddress | -
destination | ipv4 destination ipaddress | -
dscp | ipv4 dscp value | -
ecn | ipv4 ecn value | -
ttl | ipv4 ttl value | -
IP_MASK_LEN | mask length for ipv4 address | 1-32

Command Mode
IPFIX recorder Configuration

Default
Default value is 32

Usage
None

Examples
This example shows how to configure to use ipv4 source address and ipv4 destination address in ipfix recorder:
Switch# configure terminal
Switch(config)# ipfix recorder recorder1
Switch(Config-ipfix-recorder)# match ipv4 source address
Switch# configure terminal
Switch(config)# ipfix recorder recorder1
Switch(Config-ipfix-recorder)# match ipv4 destination address

Related Commands
None

15.8.4 match ipv6

Command Purpose
This command configures the fields of ipv6 in ipfix recorder, use the no form of this command to delete this configure.

Command Syntax
match ipv6 ( source | destination ) address ( mask IPV6_MASK_LEN )
no match ipv6 ( source | destination ) address
match ipv6 ( flowlabel | dscp )
no match ipv6 (flowlabel | dscp)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>ipv6 source ipaddress</td>
<td>-</td>
</tr>
<tr>
<td>destination</td>
<td>ipv4 destination ipaddress</td>
<td>-</td>
</tr>
<tr>
<td>dscp</td>
<td>ipv6 dscp value</td>
<td>-</td>
</tr>
<tr>
<td>flowlabel</td>
<td>ipv6 flowlabel value</td>
<td>-</td>
</tr>
<tr>
<td>IPV6_MASK_LEN</td>
<td>mask length for ipv6 address</td>
<td>range is 1-128 and must be the multiple of 4</td>
</tr>
</tbody>
</table>

**Command Mode**

IPFIX recorder Configuration

**Default**

Default value is 128

**Usage**

None

**Examples**

This example shows how to configure to use ipv6 source address and ipv6 destination address in ipfix recorder:

```
Switch# configure terminal
Switch(config)# ipfix recorder recorder1
Switch(Config-ipfix-recorder)# match ipv6 source address

Switch# configure terminal
Switch(config)# ipfix recorder recorder1
Switch(Config-ipfix-recorder)# match ipv6 destination address
```

**Related Commands**

None

15.8.5 match mac

**Command Purpose**

This command configures the fields of mac in ipfix recorder, use the no form of this command to delete this configure.

**Command Syntax**

```
macth mac (destination|source) address
no match mac (destination|source) address
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>Source mac address</td>
<td>-</td>
</tr>
<tr>
<td>destination</td>
<td>Destination mac address</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

IPFIX recorder Configuration
Default
None

Usage
None

Examples
This example shows how to configure to use source mac address in ipfix recorder:
Switch# configure terminal
Switch(config)# ipfix recorder recorder1
Switch(Config-ipfix-reocrder)# match mac source address

Related Commands
None

15.8.6 match transport

Command Purpose
This command configures the fields of transport in ipfix recorder, use the no form of this command to delete this configure.

Command Syntax
match transport ( destination-port | source-port | type )
no match transport ( destination-port | source-port | type )
match transport icmp ( opcode | type )
no match transport icmp ( opcode | type )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination-port</td>
<td>Destination port</td>
<td>-</td>
</tr>
<tr>
<td>source-port</td>
<td>Source port</td>
<td>-</td>
</tr>
<tr>
<td>type</td>
<td>Transport layer type</td>
<td>-</td>
</tr>
<tr>
<td>opcode</td>
<td>Icmp operated code</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
IPFIX recorder Configuration

Default
None

Usage
None

Examples
This example shows how to configure to use source port and destination port of transport in ipfix recorder:
Switch# configure terminal
Switch(config)# ipfix recorder recorder1
Switch(Config-ipfix-reocrder)# match transport source-port

Switch# configure terminal
Switch(config)# ipfix recorder recorder1
Switch(Config-ipfix-reocrder)# match transport destination-port

Related Commands
None
15.8.7 match vlan

Command Purpose
This command configures the fields of vlan in ipfix recorder, use the no form of this command to delete this configure.

Command Syntax
match vlan (inner | )
no match vlan (inner | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>inner</td>
<td>Inner VLAN</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
IPFIX recorder Configuration

Default
None

Usage
None

Examples
This example shows how to configure to use inner vlan in ipfix recorder:
Switch# configure terminal
Switch(config)# ipfix recorder recorder1
Switch(Config-ipfix-recorder)# match vlan inner

Related Commands
None

15.8.8 match cos

Command Purpose
This command configures the fields of cos in ipfix recorder, use the no form of this command to delete this configure.

Command Syntax
match cos (inner | )
no match cos (inner | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>inner</td>
<td>Inner COS</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
IPFIX recorder Configuration

Default
None

Usage
None
Examples

This example shows how to configure to use inner cos in ipfix recorder:
Switch# configure terminal
Switch(config)# ipfix recorder recorder1
Switch(Config-ipfix-reocrder)# match cos inner

Related Commands

None

15.8.9 match interface (input | output)

Command Purpose

This command configures the fields of interface in ipfix recorder, use the no form of this command to delete this configure.

Command Syntax

match interface (input | output )
no match interface (input | output )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>input</td>
<td>input direction</td>
<td>-</td>
</tr>
<tr>
<td>output</td>
<td>output direction</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

IPFIX recorder Configuration

Default

None

Usage

None

Examples

This example shows how to configure input direction in ipfix recorder:
Switch# configure terminal
Switch(config)# ipfix recorder recorder1
Switch(Config-ipfix-reocder)# match interface input

Related Commands

None

15.8.10 match vxlan-vni

Command Purpose

This command configures the fields of vxlan-vni in ipfix recorder, use the no form of this command to delete this configure.

Command Syntax

match vxlan-vni
no match vxlan-vni

Command Mode

IPFIX recorder Configuration
Default
None

Usage
None

Examples
This example shows how to configure to use vxlan-vni in ipfix recorder:
Switch# configure terminal
Switch(config)# ipfix recorder recorder1
Switch(Config-ipfix-recorder)# match vxlan-vni

Related Commands
None

15.8.11 match nvgre-key

Command Purpose
This command configures the fields of nvgre-key in ipfix recorder, use the no form of this command to delete this configure.

Command Syntax
match nvgre-key
no match nvgre-key

Command Mode
IPFIX recorder Configuration

Default
None

Usage
None

Examples
This example shows how to configure to use nvgre-key in ipfix recorder:
Switch# configure terminal
Switch(config)# ipfix recorder recorder1
Switch(Config-ipfix-recorder)# match nvgre-key

Related Commands
None

15.8.12 match packet (drop | non-drop)

Command Purpose
This command configures the fields of packet in ipfix recorder, use the no form of this command to delete this configure.

Command Syntax
match packet ( drop | non-drop )
no match packet ( drop | non-drop )
### Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>drop</td>
<td>Drop packet</td>
<td>-</td>
</tr>
<tr>
<td>non-drop</td>
<td>Non-drop packet</td>
<td>-</td>
</tr>
</tbody>
</table>

### Command Mode

IPFIX recorder Configuration

### Default

None

### Usage

None

### Examples

This example shows how to configure to use drop packet:

```
Switch# configure terminal
Switch(config)# ipfix recorder recorder1
Switch(Config-ipfix-recorder)# match packet drop
```

### Related Commands

None

#### 15.8.13 collect counter

### Command Purpose

This command configures byte number and packet number that needed to be collected in ipfix recorder, use the no form of this command to delete this configure.

### Command Syntax

```
collect counter (bytes | packets)
no collect counter (bytes | packets)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>bytes</td>
<td>Collect flow with byte number</td>
<td>-</td>
</tr>
<tr>
<td>packets</td>
<td>Collect flow with packet number</td>
<td>-</td>
</tr>
</tbody>
</table>

### Command Mode

IPFIX recorder Configuration

### Default

None

### Usage

None

### Examples

This example shows how to configure to collect the number of flow's byte in ipfix recorder:

```
Switch# configure terminal
Switch(config)# ipfix recorder recorder1
Switch(Config-ipfix-recorder)# collect counter bytes
```
Related Commands

None

15.8.14 collect flow

Command Purpose

This command configures to collect ipfix flow information in ipfix recorder, use the no form of this command to delete this configure.

Command Syntax

collect flow ( drop | destination | fragmentation )
no collect flow ( drop | destination | fragmentation )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>drop</td>
<td>Only collect the dropped flows</td>
<td>-</td>
</tr>
<tr>
<td>destination</td>
<td>Collect destination address of flows</td>
<td>-</td>
</tr>
<tr>
<td>fragmentation</td>
<td>Only collect the fragmented flows</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

IPFIX recorder Configuration

Default

None

Usage

None

Examples

This example shows how to configure to collect the destination address of flows in ipfix recorder:

Switch# configure terminal
Switch(config)# ipfix recorder recorder1
Switch(Config-ipfix-recorder)# collect flow destination

Related Commands

None

15.8.15 collect ttl

Command Purpose

This command configures to collect ipfix flow information about ttl in ipfix recorder, use the no form of this command to delete this configure.

Command Syntax

collect ttl ( maximum | minimum | changed )
no collect ttl ( maximum | minimum | changed )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>maximum</td>
<td>Collect flow max ttl value</td>
<td>-</td>
</tr>
<tr>
<td>minimum</td>
<td>Collect flow min ttl value</td>
<td>-</td>
</tr>
<tr>
<td>changed</td>
<td>Collect flow ttl changed history</td>
<td>-</td>
</tr>
</tbody>
</table>
**Command Mode**

IPFIX recorder Configuration

**Default**

None

**Usage**

None

**Examples**

This example shows how to configure to collect the maximum ttl and minimum ttl of the flows in ipfix recorder:

Switch# configure terminal
Switch(config)# ipfix recorder recorder1
Switch(Config-ipfix-recorder)# collect ttl maximum
Switch(Config-ipfix-recorder)# collect ttl minimum

**Related Commands**

None

**15.8.16 collect timestamp**

**Command Purpose**

This command configures to collect ipfix flow information about timestamp in ipfix recorder, use the no form of this command to delete this configure.

**Command Syntax**

```plaintext
collect timestamp (first | last)  
no collect timestamp (first | last)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>first</td>
<td>Collect flow start timestamp</td>
<td>-</td>
</tr>
<tr>
<td>last</td>
<td>Collect flow end timestamp</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

IPFIX recorder Configuration

**Default**

None

**Usage**

None

**Examples**

This example shows how to configure to collect the timestamp of the flows in ipfix recorder:

Switch# configure terminal
Switch(config)# ipfix recorder recorder1
Switch(Config-ipfix-recorder)# collect timestamp first

**Related Commands**

None
15.8.17 ipfix exporter

Command Purpose
Use this command to create an ipfix exporter and enter exporter configure mode. To remove the ipfix exporter, use the no form of this command.

Command Syntax

ipfix exporter NAME
no ipfix exporter NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>ipfix exporter name</td>
<td>Up to 32 characters</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
If ipfix exporter has existed, it will enter IPFIX exporter Configuration; if ipfix exporter is new, it will create exporter and enter IPFIX exporter Configuration; this command should work with the other commands.

Examples
This example shows how to create ipfix exporter exporter1 in global configuration and enter IPFIX exporter Configuration:

```
Switch# configure terminal
Switch(config)# ipfix exporter exporter1
```

This example shows how to delete ipfix exporter exporter1:

```
Switch# configure terminal
Switch(config)# no ipfix exporter exporter1
```

Related Commands
template data timeout
flow data timeout
event flow start
event flow end (tcp-end|timeout)
transport protocol (udp|tcp)

15.8.18 description

Command Purpose
This command used to describe ipfix exporter; use the no form of this command to delete this description.

Command Syntax
description DESCRIPTION

description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DESCRIPTION</td>
<td>Ipfix exporter description</td>
<td>Up to 64 characters</td>
</tr>
</tbody>
</table>

Command Mode
IPFIX exporter Configuration
**Default**
None

**Usage**
None

**Examples**

```
Switch# configure terminal
Switch(config)# ipfix exporter exporter1
Switch(Config-ipfix-exporter)# description this is a ipfix exporter
```

```
Switch# configure terminal
Switch(config)# ipfix exporter exporter1
Switch(Config-ipfix-exporter)# no description
```

**Related Commands**
None

**15.8.19 destination**

**Command Purpose**
This command used to configure collector host name that need to receive flow records in ipfix exporter, use the no form of this command to delete this description.

**Command Syntax**

```
destination HOST
no destination HOST
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOST</td>
<td>The length of host name should not exceed 32 characters</td>
<td>Up to 32 characters</td>
</tr>
</tbody>
</table>

**Command Mode**
IPFIX exporter Configuration

**Default**
None

**Usage**
None

**Examples**

This example shows how to create a host named host1 in IPFIX exporter Configuration:

```
Switch# configure terminal
Switch(config)# ipfix exporter exporter1
Switch(config)# ipfix exporter exporter1# destination host1
```

**Related Commands**
None

**15.8.20 dscp**

**Command Purpose**
this command used to configure the dscp value of the message that need to be sended in ipfix exporter, use the no form of this command to delete this description.
**Command Syntax**

dscp DSCP

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP</td>
<td>dscp value</td>
<td>0-63</td>
</tr>
</tbody>
</table>

**Command Mode**

IPFIX exporter Configuration

**Default**

None

**Usage**

None

**Examples**

This example shows how to configure dscp to be 20 in IPFIX exporter Configuration:

Switch# configure terminal
Switch(config)# ipfix exporter exporter1
Switch(Config-ipfix-exporter)# dscp 20

**Related Commands**

None

**15.8.21 domain-id**

**Command Purpose**

This command used to configure the ipfix domain value of the message that needs to be sent in ipfix exporter, use the no form of this command to delete this description.

**Command Syntax**

domain-id ID

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>domain id</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

**Command Mode**

IPFIX exporter Configuration

**Default**

None

**Usage**

None

**Examples**

This example shows how to configure domain-id to be 1000 in IPFIX exporter Configuration:

Switch# configure terminal
Switch(config)# ipfix exporter exporter1
Switch(Config-ipfix-exporter)# domain-id 1000
Related Commands
None

15.8.22  source interface

Command Purpose
This command used to configure which interface should send ipfix record in ipfix exporter, use the no form of this command to delete this description.

Command Syntax
source interface interface-number
no source interface-number

Command Mode
IPFIX exporter Configuration

Default
None

Usage
None

Examples
This example shows how to configure use interface eth-0-1 to send ipfix records in IPFIX exporter Configuration:
Switch# configure terminal
Switch(config)# ipfix exporter exporter1
Switch(Config-ipfix-exporter)# source interface eth-0-1

Related Commands
None

15.8.23  template data timeout

Command Purpose
This command used to configure time interval of sending template data in ipfix exporter, use the no form of this command to delete this description.

Command Syntax
template data timeout TIMEOUT
no template data timeout

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIMEOUT</td>
<td>template data timeout</td>
<td>1-86400</td>
</tr>
</tbody>
</table>

Command Mode
IPFIX exporter Configuration

Default
600

Usage
None
Examples

This example shows how to configure time interval of sending template data to be 200 seconds in IPFIX exporter Configuration:
Switch# configure terminal
Switch(config)# ipfix exporter exporter1
Switch(Config-ipfix-exporter)# template data timeout 200

Related Commands
None

15.8.24 flow data timeout

Command Purpose
This command used to configure time interval of sending flow data in ipfix exporter, use the no form of this command to delete this description.

Command Syntax
flow data timeout \textit{TIMEOUT}
no flow data timeout

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>\textit{TIMEOUT}</td>
<td>flow data timeout</td>
<td>1-86400</td>
</tr>
</tbody>
</table>

Command Mode
IPFIX exporter Configuration

Default
600

Usage
None

Examples
This example shows how to configure time interval of sending flow data to be 200 seconds in IPFIX exporter Configuration:
Switch# configure terminal
Switch(config)# ipfix exporter exporter1
Switch(Config-ipfix-exporter)# flow data timeout 200

Related Commands
None

15.8.25 transport protocol

Command Purpose
This command used to configure to use which transport when send message in ipfix exporter, use the no form of this command to delete this description.

Command Syntax
transport protocol udp port \textit{UDP\_PORT}
no transport protocol
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP_PORT</td>
<td>transport protocol number</td>
<td>Range is 2000 to 65535, Default is 2055</td>
</tr>
</tbody>
</table>

**Command Mode**

IPFIX exporter Configuration

**Default**

2055

**Usage**

None

**Examples**

This example shows how to configure transport protocol of flow data send to udp and its port is 3500 in IPFIX exporter Configuration:

Switch# configure terminal
Switch(config)# ipfix exporter exporter1
Switch(Config-ipfix-exporter)# transport protocol udp 3500

**Related Commands**

None

15.8.26 ttl

**Command Purpose**

This command used to configure the ttl of the send message in ipfix exporter. use the no form of this command to delete this description.

**Command Syntax**

ttl TTL
no ttl

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TTL</td>
<td>TTL value</td>
<td>1-255</td>
</tr>
</tbody>
</table>

**Command Mode**

IPFIX exporter Configuration

**Default**

None

**Usage**

None

**Examples**

This example shows how to configure ttl value of flow data to be 255 in IPFIX exporter Configuration:

Switch# configure terminal
Switch(config)# ipfix exporter exporter1
Switch(Config-ipfix-exporter)# ttl 255

**Related Commands**

None
15.8.27 event flow

Command Purpose
This command used to configure which event should triggle to send flow information at once in ipfix exporter. use the no form of this command to delete this description.

Command Syntax
event flow start
no event flow start
event flow end ( tcp-end | timeout )
no event flow end ( tcp-end | timeout )

Command Mode
IPFIX exporter Configuration

Default
None

Usage
None

Examples
This example shows how to configure the event about ending tcp transmission of flow data will triggle to send flow information in IPFIX exporter Configuration:
Switch# configure terminal
Switch(config)# ipfix exporter exporter1
Switch(Config-ipfix-exporter)# event flow tcp-end

Related Commands
None

15.8.28 ipfix sampler

Command Purpose
Use this command to create a ipfix sampler and enter sampler configure mode. To remove the ipfix sampler, use the no form of this command.

Command Syntax
ipfix sampler NAME
no ipfix sampler NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>ipfix sampler name</td>
<td>Up to 32 characters</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
If ipfix sampler has existed. it will enter IPFIX sampler Configuration; if ipfix sampler is new. it will create sampler and enter IPFIX sampler Configuration; this command should work with the command of match and collect.
Examples

This example shows how to create ipfix sampler sampler1 in global configuration and enter IPFIX sampler Configuration:
Switch# configure terminal
Switch(config)# ipfix sampler sampler1
Switch(Config-ipfix-sampler)#
This example shows how to delete ipfix sampler sampler1:
Switch# configure terminal
Switch(config)# no ipfix sampler sampler1

Related Commands
1 out-of

15.8.29 description

Command Purpose
This command used to describe ipfix sampler. use the no form of this command to delete this description.

Command Syntax
description DESCRIPTION

```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DESCRIPTION</td>
<td>ipfix sampler description</td>
<td>Up to 64 characters</td>
</tr>
</tbody>
</table>
```

Command Mode
IPFIX sampler Configuration

Default
None

Usage
None

Examples
Switch# configure terminal
Switch(config)# ipfix sampler sampler 1
Switch(Config-ipfix-sampler)# description this is a ipfix sampler

Switch# configure terminal
Switch(config)# ipfix sampler sampler 1
Switch(Config-ipfix-sampler)# no description

Related Commands
None

15.8.30 1 out-of

Command Purpose
This command used to configure the rate of ipfix sampler. use the no form of this command to delete this configure.

Command Syntax
1 out of CLI_IPFIX_SAMPLER_RATE_RNG
### Command Mode

**IPFIX sampler Configuration**

**Default**

None

**Usage**

None

**Examples**

This example shows how to configure the rate of sampling is 1/100 in IPFIX sampler Configuration:

```
Switch# configure terminal
Switch(config)# ipfix sampler sampler 1
Switch(Config-ipfix-sampler)# 1 out of 100
```

**Related Commands**

None

15.8.31 ipfix monitor (global)

**Command Purpose**

Use this command to create a ipfix monitor and enter monitor configure mode. To remove the ipfix monitor, use the no form of this command.

**Command Syntax**

```
ipfix monitor NAME
no ipfix monitor NAME
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>ipfix monitor name</td>
<td>Up to 32 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

**Global Configuration**

**Default**

None

**Usage**

None

**Examples**

This example shows how to create ipfix recorder recorder1 in global configuration and enter IPFIX recorder Configuration:

```
Switch# configure terminal
Switch(config)# ipfix monitor monitor1
Switch(Config-ipfix-monitor)#
```

This example shows how to delete ipfix monitor monitor1:

```
Switch# configure terminal
Switch(config)# no ipfix monitor monitor1
```

www.fs.com
Related Commands

Recorder
Exporter

15.8.32 description

Command Purpose

This command used to describe ipfix monitor. use the no form of this command to delete this description.

Command Syntax

description DESCRIPTION

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DESCRIPTION</td>
<td>The length of ipfix monitor description should not exceed 64 characters</td>
<td>Up to 64 characters</td>
</tr>
</tbody>
</table>

Command Mode

IPFIX monitor Configuration

Default

None

Usage

None

Examples

Add description for IPFIX monitor:
Switch# configure terminal
Switch(config)# ipfix monitor monitor1
Switch(Config-ipfix-monitor)# description this is a ipfix monitor

Remove description:
Switch# configure terminal
Switch(config)# ipfix monitor monitor1
Switch(Config-ipfix-monitor)# no description

Related Commands

None

15.8.33 recorder

Command Purpose

Use this command to create a ipfix recorder of the ipfix monitor. To remove the ipfix monitor, use the no form of this command.

Command Syntax

recorder NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>ipfix recorder name</td>
<td>Up to 32 characters</td>
</tr>
</tbody>
</table>

Command Mode

IPFIX monitor Configuration
**15.8.34 exporter**

**Command Purpose**

Use this command to create a ipfix exporter of the ipfix monitor. To remove the ipfix monitor, use the no form of this command.

**Command Syntax**

```
exporter NAME
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>ipfix exporter name</td>
<td>Up to 32 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

IPFIX monitor Configuration

**Default**

None

**Usage**

None

**Examples**

This example shows how to create a exporter of the ipfix monitor configure mode:

```
Switch# configure terminal
Switch(config)# ipfix monitor monitor1
Switch(Config-ipfix-monitor)# exporter exporter1
```

**Related Commands**

None

**15.8.35 ipfix monitor (interface/port-group/vlan group)**

**Command Purpose**

This command used to enable ipfix.

**Command Syntax**

```
ipfix monitor ( input | output ) NAME ( sampler NAME | )
no ipfix monitor ( input | output )
```
### Command Mode

Interface Configuration  
Port-group Configuration  
Vlan-group Configuration  

**Default**

None  

**Usage**

None  

**Examples**

This example shows how to enable ipfix:

Switch# configure terminal  
Switch(config)# interface eth-0-1  
Switch(config-if)# ipfix monitor input monitor sampler test-sample  

**Related Commands**

None  

15.8.36 ipfix global flow

**Command Purpose**

this command used to configure ipfix globally.

**Command Syntax**

ipfix global flow aging CLI_IPFIX_AGING_INTVAL_RNG  
ipfix global flow sampler ( all | new )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI_IPFIX_AGING_INTVAL_RNG</td>
<td>The aging time of the flow</td>
<td>Range is 1 to 65535, the default is 1800 seconds</td>
</tr>
<tr>
<td>all</td>
<td>All the packets can be counted to the sampling sum</td>
<td>-</td>
</tr>
<tr>
<td>new</td>
<td>Only the new packets can be counted to the sampling sum</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration  

**Default**

None
Usage
None

Examples
This example shows how to configure the aging time to be 200 seconds in global configure mode:
Switch# configure terminal
Switch(config)# ipfix global flow aging 200

Related Commands
None

15.8.37 show ipfix recorder

Command Purpose
Use the show ipfix recorder privileged EXEC command to display the configure information of one ipfix recorder.

Command Syntax
show ipfix recorder NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>ipfix recorder name</td>
<td>Up to 32 characters</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to show ipfix recorder command:
Switch# show ipfix recorder recorder1

Related Commands
None

15.8.38 show ipfix exporter

Command Purpose
Use the show ipfix exporter privileged EXEC command to display the configure information of one ipfix exporter.

Command Syntax
show ipfix exporter NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>ipfix exporter name</td>
<td>Up to 32 characters</td>
</tr>
</tbody>
</table>
Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to display configuration about exporter1 in privileged EXEC mode:
Switch# show ipfix exporter exporter1

Related Commands
None

15.8.39 show ipfix cache

Command Purpose
This command used to show the state information of the ipfix on the interface.

Command Syntax
show ipfix cache interface IFNAME (input | output) ( detail | )
show ipfix cache counter ( interface IFNAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical ports</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to show the state information of the ipfix on the interface eth-0-1 in privileged EXEC mode:
Switch# show ipfix cache interface eth-0-1 input detail

Related Commands
None

15.8.40 show ipfix monitor

Command Purpose
This command used to describe the configuration of the ipfix monitor.

Command Syntax
show ipfix monitor NAME
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>ipfix monitor name</td>
<td>Up to 32 characters</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
This example shows how to display configuration of monitor 1 in privileged EXEC mode:

```
Switch# show ipfix monitor monitor 1
```

**Related Commands**
None

**15.8.41 show ipfix sampler**

**Command Purpose**
This command used to describe the configuration of the ipfix sampler.

**Command Syntax**

```
show ipfix sampler NAME
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>ipfix sampler name</td>
<td>Up to 32 characters</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
This example shows how to display configuration of sampler1 in privileged EXEC mode:

```
Switch# show ipfix sampler sampler1
```

**Related Commands**
None
15.8.42 clear ipfix cache monitor

**Command Purpose**
This command used to clear cache with ipfix monitor name.

**Command Syntax**
clear ipfix cache monitor NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>IPFIX monitor name</td>
<td>Up to 32 characters</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
This example shows how to clear ipfix cache with name test in privileged EXEC mode:
Switch# clear ipfix cache monitor test

**Related Commands**
None

15.8.43 clear ipfix cache observe-point interface

**Command Purpose**
This command used to clear cache on interface.

**Command Syntax**
clear ipfix cache observe-point interface (IFNAME) (input | output)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFPHYSICAL</td>
<td>Name of interface</td>
<td>Support physical/aggregation/VLAN ports</td>
</tr>
<tr>
<td>input</td>
<td>the inputed packets</td>
<td>-</td>
</tr>
<tr>
<td>output</td>
<td>the outputed packets</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None
Examples

This example shows how to clear ipfix cache on interface eth-0-1 in privileged EXEC mode:
Switch# clear ipfix cache observe-point interface eth-0-1 input

Related Commands

None
Chapter 16 VPN Commands

16.1 VRF Commands

16.1.1 ip vrf

Command Purpose
To configure a VPN routing and forwarding (VRF) routing table, use the ip vrf command in global configuration mode. To remove a VRF routing table, use the no form of this command.

Command Syntax
ip vrf VRF-NAME
no ip vrf VRF-NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF-NAME</td>
<td>VPN Routing/Forwarding instance name</td>
<td>Up to 15 characters</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
None

Examples
Switch# configure terminal
Switch(config)# ip vrf ComA
Switch(config-vrf)# route-target both 100:2
Switch(config-vrf)# route-target import 200:1

Related Commands
ip vrf forwarding

16.1.2 show ip vrf

Command Purpose
To show the set of defined VRFs and associated interfaces, use the show ip vrf command in Privileged EXEC mode.
Command Syntax

show ip vrf ( bgp ( brief | detail ) | interfaces | ospf | rip | VRF-NAME )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp</td>
<td>Border Gateway Protocol (BGP)</td>
<td>-</td>
</tr>
<tr>
<td>brief</td>
<td>Brief VPN Routing/Forwarding instance information</td>
<td>-</td>
</tr>
<tr>
<td>detail</td>
<td>Detailed VPN Routing/Forwarding instance information</td>
<td>-</td>
</tr>
<tr>
<td>interfaces</td>
<td>Show VPN Routing/Forwarding interface information</td>
<td>-</td>
</tr>
<tr>
<td>ospf</td>
<td>Open Shortest Path First (OSPF)</td>
<td>-</td>
</tr>
<tr>
<td>rip</td>
<td>Routing Information Protocol (RIP)</td>
<td>-</td>
</tr>
<tr>
<td>VRF-NAME</td>
<td>VPN Routing/Forwarding instance name</td>
<td>Up to 15 characters</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

Switch# show ip vrf

Related Commands

None

16.1.3 ip vrf forwarding

Command Purpose
To associate a VPN routing and forwarding (VRF) instance with an Layer3 interface, use the ip vrf forwarding command in interface configuration mode. To disassociate a VRF, use the no form of this command.

Command Syntax

ip vrf forwarding VRF-NAME
no ip vrf forwarding
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF-NAME</td>
<td>VPN Routing/Forwarding instance name</td>
<td>Up to 15 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

None

**Usage**

Executing this command on an interface removes the IP address on this interface. The IP address should be reconfigured.

**Examples**

```
Switch# configure terminal
Switch(config)# ip vrf ComA
Switch(config-vrf)# exit
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip vrf forwarding ComA
```

**Related Commands**

- ip vrf
- ip route vrf

### 16.1.4 ip route vrf

**Command Purpose**

To establish static routes for a VPN routing and forwarding (VRF) instance, use the `ip route vrf` command in global configuration mode. To remove static routes, use the `no` form of this command.

**Command Syntax**

```
ip route vrf VRF-NAME DST_NET NH_ADDR
nip route vrf VRF-NAME DST_NET NH_ADDR
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF-NAME</td>
<td>VPN Routing/Forwarding instance name</td>
<td>Up to 15 characters</td>
</tr>
<tr>
<td>DST_NET</td>
<td>Destination IP subnet, the format can be target IP address with masklen(A.B.C.D/M) or target IP address with netmask (A.B.C.D A.B.C.D)</td>
<td>The format can be target IP address with masklen(A.B.C.D/M) or target IP address with netmask (A.B.C.D A.B.C.D)</td>
</tr>
<tr>
<td>NH_ADDR</td>
<td>Next-hop IP address, the format should be A.B.C.D</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>
Command Mode

Global Configuration

Default

None

Usage

None

Examples

Switch# configure terminal
Switch(config)# ip route vrf VPN-NAME 2.2.2.0/24 1.1.1.2

Related Commands

show ip route vrf

16.1.5 arp vrf

Command Purpose

To add a permanent entry in the Address Resolution Protocol (ARP) cache for VRF, use the arp vrf command in global configuration mode. To remove an entry from VRF ARP cache, enter the no form of this command.

Command Syntax

arp vrf VRF_NAME IP_ADDR MAC
no arp vrf VRF_NAME IP_ADDR

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF-NAME</td>
<td>VPN Routing/Forwarding instance name</td>
<td>Up to 15 characters</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>IP address of the ARP entry</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>MAC</td>
<td>Hardware address of the ARP entry in HHHH.HHHH.HHHH format</td>
<td>MAC Address</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration
**Default**

None

**Usage**

None

**Examples**

```
Switch# configure terminal
Switch(config)# arp vrf vpn3 1.1.1.1 0000.1111.2222
```

**Related Commands**

show ip arp vrf VRF-NAME
clear ip arp vrf VRF-NAME A.B.C.D

16.1.6 show ip arp vrf

**Command Purpose**

Use this command to show arp entry in VRF instance.

**Command Syntax**

```
show ip arp vrf VRF-NAME
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF-NAME</td>
<td>VPN Routing/Forwarding instance name</td>
<td>Up to 15 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None
Examples

This example shows how to display all arp entry in the arp table of the VRF:

Switch# show ip arp vrf ComA

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Address</th>
<th>Age (min)</th>
<th>Hardware Addr</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet</td>
<td>1.1.1.1</td>
<td>-</td>
<td>0000.1111.2222</td>
<td></td>
</tr>
</tbody>
</table>

Related Commands

arp vrf

16.1.7 clear ip arp vrf

Command Purpose

Use this command to refresh a specific dynamic ARP entry from ARP cache for the VRF.

Command Syntax

clear ip arp vrf VRF-NAME IP_ADDR

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF-NAME</td>
<td>VPN Routing/Forwarding instance name</td>
<td>Up to 15 characters</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>Dynamic learned ARP entry IP address</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to refresh a dynamic arp entry in VRF:

Switch# clear ip arp vrf ComA 1.1.1.1
Related Commands

arp vrf

16.1.8 ping vrf

Command Purpose

Use this command to ping address in VRF.

Command Syntax

ping vrf VRF-NAME IPV4_HOST

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF-NAME</td>
<td>VPN Routing/Forwarding instance name</td>
<td>-</td>
</tr>
<tr>
<td>IPV4_HOST</td>
<td>Ping destination address or hostname</td>
<td>IPv4 Address or host name string</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

Switch# ping vrf vpn 1.1.1.1

PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=0 ttl=64 time=0.114 ms
64 bytes from 1.1.1.1: icmp_seq=1 ttl=64 time=0.087 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=64 time=0.087 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=64 time=0.097 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=64 time=0.133 ms
--- 1.1.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4041ms
rtt min/avg/max/mdev = 0.087/0.103/0.133/0.020 ms, pipe 2
16.1.9 traceroute vrf

Command Purpose
Use this command to trace route in VRF.

Command Syntax
traceroute vrf VRF-NAME IPV4_HOST

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF-NAME</td>
<td>VPN Routing/Forwarding instance name</td>
<td>Up to 15 characters</td>
</tr>
<tr>
<td>WORD</td>
<td>Trace route destination address or hostname</td>
<td>IPv4 Address or host name string</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
Switch# traceroute vrf vpn 1.1.1.1
traceroute to 1.1.1.1 (1.1.1.1), 30 hops max, 38 byte packets
  1 1.1.1.1 (1.1.1.1)    0.222 ms    0.169 ms    0.169 ms

16.1.10 telnet vrf

Command Purpose
Use this command to telnet in VRF.

Command Syntax
telnet vrf VRF-NAME WORD

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF-NAME</td>
<td>VPN Routing/Forwarding instance name</td>
<td>Up to 15 characters</td>
</tr>
<tr>
<td>WORD</td>
<td>The destination address or hostname for telnet</td>
<td>-</td>
</tr>
</tbody>
</table>
Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

Switch# telnet vrf vpn 9.9.9.2

Trying 9.9.9.2...
Connected to 9.9.9.2.
Escape character is '^]'.
Fedora Core release 4 (Stentz)
Kernel 2.6.32.23 on an i686
login: root
Password:

Related Commands

None

16.1.11 rd

Command Purpose

Use this command to set route distinguisher.

Command Syntax

rd RD-VALUE

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RD-VALUE</td>
<td>Route distinguisher value. ASN:nn or IPv-address:nn</td>
<td>The range of ASN is 1-4294967295 or in IPv4 format. The range of nn is 1-65535</td>
</tr>
</tbody>
</table>

Command Mode

VRF Configuration
**Default**

None

**Usage**

None

**Examples**

```
Switch# configure terminal
Switch(config)# ip vrf test
Switch(config-vrf)# rd 1.1.1.1:1
```

**Related Commands**

None

**16.1.12 route-target**

**Command Purpose**

Use this command to set route target. To unset route target, enter the no form of this command.

**Command Syntax**

```
route-target ( both | export | import ) RT-VALUE
no route-target ( both | export | import ) ( RT-VALUE )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>both</td>
<td>Import and export</td>
<td>-</td>
</tr>
<tr>
<td>export</td>
<td>Export</td>
<td>-</td>
</tr>
<tr>
<td>import</td>
<td>Import</td>
<td>-</td>
</tr>
<tr>
<td><strong>RT-VALUE</strong></td>
<td>Route-target value. ASN:nn or IP-address:nn</td>
<td>The range of ASN is 1-4294967295 or in IPv4 format, The range of nn is 1-65535</td>
</tr>
</tbody>
</table>

**Command Mode**

VRF Configuration

**Default**

None
Usage

None

Examples

Switch# configure terminal
Switch(config)# ip vrf test
Switch(config-vrf)# route-target import 100:1

Related Commands

None

16.1.13 import map

Command Purpose

Use this command to set import map. To unset import map, enter the no form of this command.

Command Syntax

import map WORD
no import map

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>Pointer to route-map entries</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode

VRF Configuration

Default

None

Usage

None

Examples

Switch# configure terminal
Switch(config)# ip vrf test
Switch(config-vrf)# import map 100

Related Commands

export map
16.1.14 export map

Command Purpose

Use this command to set export map. To unset export map, enter the no form of this command.

Command Syntax

export map WORD
no export map

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>Pointer to route-map entries</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode

VRF Configuration

Default

None

Usage

None

Examples

Switch# configure terminal
Switch(config)# ip vrf test
Switch(config-vrf)# export map 100

Related Commands

import map

16.1.15 router-id

Command Purpose

Use this command to set router-id. To unset router-id, enter the no form of this command.

Command Syntax

router-id IP_ADDR
no router-id

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>Router identifier in IP address format</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

**Command Mode**

**VRF Configuration**

**Default**

None

**Usage**

None

**Examples**

Switch# configure terminal
Switch(config)# ip vrf test
Switch(config-vrf)# router-id 1.1.1.1

**Related Commands**

show ip vrf

**16.1.16 description**

**Command Purpose**

Use this command to specific VRF description. To remove VRF description, enter the no form of this command.

**Command Syntax**

description LINE

no description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LINE</td>
<td>Characters describing this VRF</td>
<td>The name length should be no more than 40 and the first character must be a-z, A-Z or 0-9.</td>
</tr>
</tbody>
</table>

**Command Mode**

VRF Configuration
Default
None

Usage
None

Examples

Switch# configure terminal
Switch(config)# ip vrf test
Switch(config-vrf)# description VrfName1

Related Commands

show ip vrf

16.2 GRE TUNNEL Commands

16.2.1 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TUNNEL_ID</td>
<td>tunnel id</td>
<td>0-1023</td>
</tr>
</tbody>
</table>

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

16.2.2 tunnel mode gre

Command Purpose

This command 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 encapsed 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

16.2.3 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>specify a tunnel source in the IPv4 address format</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IFNAME</td>
<td>specify a tunnel source in the IFNAME format, the IFNAME should be layer3 interface, like routed port, vlan interface, loopback.</td>
<td>Support physical/aggregation/loopback/vlan ports</td>
</tr>
</tbody>
</table>

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

16.2.4 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>Specify the tunnel destination IPv4 address</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

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

16.2.5 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 )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enable tunnel packet decapsulation</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>Disable tunnel packet decapsulation</td>
<td>-</td>
</tr>
</tbody>
</table>

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

16.2.6 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

16.2.7  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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP</td>
<td>The outer IPv4 header DSCP value</td>
<td>0-63</td>
</tr>
</tbody>
</table>

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
16.2.8 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERIOD_VALUE</td>
<td>Interval period</td>
<td>1-32767</td>
</tr>
<tr>
<td>RETRY_VALUE</td>
<td>timeout and retry</td>
<td>1-255</td>
</tr>
</tbody>
</table>

**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

16.2.9 show interface tunnel

**Command Purpose**
Use this command to display the tunnel information.

**Command Syntax**
show interface tunnel TUNNEL_ID

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TUNNEL_ID</td>
<td>The tunnel ID</td>
<td>0-1023</td>
</tr>
</tbody>
</table>

**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

16.2.10 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

<table>
<thead>
<tr>
<th>Tunnel Resource</th>
<th>Used</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peers</td>
<td>0</td>
<td>8</td>
</tr>
</tbody>
</table>

Related Commands

16.2.11 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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TUNNEL_ID</td>
<td>tunnel id</td>
<td>0-1023</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example displays the statistics of gre tunnel keepalive:

Switch# show tunnel keepalive statistics

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Keepalive</th>
<th>Out_ka_pkt</th>
<th>In_ka_pkt</th>
<th>TunnelUp</th>
<th>TunnelDown</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

DUT1#
Related Commands

clear tunnel keepalive statistics

16.2.12 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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TUNNEL_ID</td>
<td>tunnel id</td>
<td>0-1023</td>
</tr>
</tbody>
</table>

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

16.2.13 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 )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TUNNEL_ID</td>
<td>tunnel id</td>
<td>0-1023</td>
</tr>
</tbody>
</table>

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

16.3 ERSPAN TUNNEL Commands

16.3.1 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TUNNEL_ID</td>
<td>tunnel id</td>
<td>0-1023</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
None

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

Related Commands
show interface tunnel
16.3.2 tunnel mode erspan

Command Purpose

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

Command Syntax

tunnel mode (erspan (ecmp-dst-gre | ) )

no tunnel mode

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>erspan</td>
<td>The tunnel mode is erspan, it has only one tunnel destination. Now, it supports IPv4 erspan tunnel, the payload packet should be IPv4 packet.</td>
<td>-</td>
</tr>
<tr>
<td>erspan ecmp-dst-gre</td>
<td>The tunnel mode is erspan, it has a certain of tunnel destinations. Now, it supports IPv4 erspan tunnel, the payload packet should be IPv4 packet.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

None

Usage

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

Examples

When configure the tunnel mode with erspan, and then it is required configure tunnel source and tunnel destination manually:

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

Related Commands

tunnel source
tunnel destination

16.3.3 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>specify a tunnel source in the IPv4 address format</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IFNAME</td>
<td>specify a tunnel source in the IFNAME format, the IFNAME should be layer3 interface, like routed port, vlan interface, loopback.</td>
<td>Support physical/aggregation/loopback/vlan ports</td>
</tr>
</tbody>
</table>

## Command Mode

Interface Configuration

## Default

None

## Usage

None

## Examples

Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel source 3.3.3.3

## Related Commands

tunnel mode erspan
tunnel destination

### 16.3.4  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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>Specify the tunnel destination IPv4 address</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

## Command Mode

Interface Configuration

## Default

None
**Usage**

None

**Examples**

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel mode erspan
Switch(config-if)# tunnel destination 4.4.4.4
```

**Related Commands**

- `tunnel source`
- `tunnel mode erspan`

### 16.3.5 tunnel ecmp-destination

**Command Purpose**

Use this command to specify tunnel ecmp-destination address in an IPv4 portion. Use the no parameter to un-specify the address.

**Command Syntax**

```
tunnel ecmp-destination IP_ADDR
no tunnel ecmp-destination IP_ADDR
no tunnel ecmp-destination all
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>tunnel ecmp-destination address</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

None

**Usage**

None

**Examples**

This example shows how to set the tunnel ecmp-destination:

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config)# tunnel mode erspan ecmp-dst-gre
Switch(config-if)# tunnel ecmp-destination 3.3.3.3
Switch(config-if)# tunnel ecmp-destination 4.4.4.4
```
Related Commands

tunnel source
tunnel mode erspan ecmp-dst-gre

16.3.6 tunnel gre key

Command Purpose
Use this command to set the key of erspan tunnel. Use the no form of this command to unset the key of erspan tunnel.

Command Syntax

```
tunnel gre key KEY_VALUE
no tunnel gre key
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEY_VALUE</td>
<td>gre key value</td>
<td>1-4294967295</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

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

Related Commands

tunnel source

16.3.7 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP</td>
<td>The outer IPv4 header DSCP value</td>
<td>0-63</td>
</tr>
</tbody>
</table>
Command Mode
Interface Configuration

Default
None

Usage
None

Examples
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel dscp 40

Related Commands
Interface

16.3.8 tunnel ttl

Command Purpose
set this command to specify a value of time to live (ttl) in the tunnel IPv4 encapsulation header. Use the no parameter to inheriting the underlying physical interface value by default.

Command Syntax
tunnel ttl TTL
no tunnel ttl

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TTL</td>
<td>The outer IPv4 header ttl value</td>
<td>1-254</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
64

Usage
None

Examples
This example shows how to set the outer IPv4 header ttl value as 40:
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel ttl 40
Related Commands
Interface

16.3.9 tunnel extend-header

Command Purpose
Use this command to set the extend-header information in erspan.

Command Syntax
- tunnel extend-header
- no tunnel extend-header

Command Mode
Interface Configuration

Default
None.

Usage
None.

Examples
This example shows how to set extend-header in erspan mode:

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel extend-header
```

Related Commands
tunnel extend-header id

16.3.10 tunnel extend-header id

Command Purpose
Use this command to set the extend-header id in erspan. Use the no form of this command can unset extend-header id in erspan.

Command Syntax
- tunnel extend-header id ID
- no tunnel extend-header id

```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>The extend-header id</td>
<td>1-1023</td>
</tr>
</tbody>
</table>
```

Command Mode
Interface Configuration
Default
None.

Usage
You must configure the tunnel extend-header before setting the extend-header id.

Examples
This example shows how to set extend-header id in erspan mode:

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel extend-header
Switch(config-if)# tunnel extend-header id 1
```

Related Commands
tunnel extend-header

16.3.11 tunnel extend-header dst-load-balance

Command Purpose
Use this command to set the extend-header dst-load-balance in erspan. Use the no form of this command can unset extend-header dst-load-balance in erspan.

Command Syntax
tunnel extend-header dst-load-balance
no tunnel extend-header dst-load-balance

Command Mode
Interface Configuration

Default
None.

Usage
None.

Examples
This example shows how to set extend-header dst-load-balance in erspan mode:

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel extend-header
Switch(config-if)# tunnel extend-header dst-load-balance
```

Related Commands
tunnel extend-header
16.3.12  show resource tunnel

Command Purpose

Use this command to show the resource usage of the tunnel.

Command Syntax

show resource tunnel

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

Switch# show resource tunnel

Tunnel
Resource  Used  Capability
Peers  3  8

Related Commands

None
Chapter 17 Data Center Commands

17.1 Overlay Commands

17.1.1 vlan overlay enable

Command Purpose
Use this command to set vlan overlay enable/disable.

Command Syntax
```
 vlan VLAN_ID overlay ( enable | disable )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan id</td>
<td>2-4094</td>
</tr>
<tr>
<td>enable</td>
<td>set the overlay feature of the VLAN to enable</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>set the overlay feature of the VLAN to disable, and it is disabled by default</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
VLAN Configuration

Default
Disable

Usage
Make sure that overlay of vlan is enabled before configure overlay vlan and vni mapping.

Examples
The following example shows how to set overlay of vlan 2 to enable:
```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# vlan 2 overlay enable
```

Related Commands
None

17.1.2 Overlay

Command Purpose
Use this command to enter overlay configure mode.
To return the configure mode, use the exit command.
Command Syntax

Overlay

Command Mode

Global Configuration

Default

None

Usage

None

Examples

The following example shows how to enter into overlay configure mode:

```
Switch# configure terminal
Switch(config)# overlay
Switch(config-overlay)#
```

Related Commands

None

17.1.3 vlan vni

Command Purpose

Use this command to mapping vlan id with overlay vni.

Command Syntax

```
vlan VLAN_ID vni VNI
```

```
no vlan VLAN_ID vni
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan id</td>
<td>2-4094</td>
</tr>
<tr>
<td>VNI</td>
<td>vni id</td>
<td>1-16777215</td>
</tr>
</tbody>
</table>

Command Mode

OVERLAY Configuration

Default

None
Usage
The overlay mapping command is used to bind the vlan id with overlay vni. That means the vlan is now can work as one overlay bridge domain and all the port belong this vlan will also be in the overlay bridge domain.

Examples
The following example set the overlay mapping:

```
Switch# configure terminal
Switch(config)# overlay
Switch(config-overlay)# vlan 20 vni 20000
```

The following example unset the overlay mapping:

```
Switch# configure terminal
Switch(config)# overlay
Switch(config-overlay)# no vlan 20 vni
```

Related Commands
None

17.1.4 vni split-horizon-disable

Command Purpose
Use this command to disable horizon split per vni. Use the no form of this command to enable horizon split per vni.

Command Syntax
```
vni VNId split-horizon-disable
no vni VNId split-horizon-disable
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VNI</td>
<td>vni id</td>
<td>1-16777215</td>
</tr>
</tbody>
</table>

Command Mode
OVERLAY Configuration

Default
Horizon split is enabled.

Usage
None

Examples
The following example shows how to disable horizon split per vni:

```
Switch# configure terminal
Switch(config)# overlay
Switch(config-overlay)# vni 20000 split-horizon-disable
```

The following example shows how to enable horizon split per vni:

```
Switch# configure terminal
Switch(config)# overlay
Switch(config-overlay)# no vni 20000 split-horizon-disable
```

Related Commands
None
17.1.5 Source

Command Purpose

Use this command to set the overlay source vtep ip address.
To remove the source vtep ip address, use the no form of this command.

Command Syntax

source IP_ADDR

no source

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>The overlay source vtep ip address, it should be a valid interface ip address.</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

Command Mode

OVERLAY Configuration

Default

None

Usage

Overlay source vtep ip address is used to encap and decap overlay packets. It is recommended that the source vtep ip address is the same with some loopback interface address so that ip routing can be reachable.

Examples

The following example sets the source vtep ip address of overlay:
Switch# configure terminal
Switch(config)# overlay
Switch(config-overlay)# source 1.1.1.1

The following example removes the source vtep ip address of overlay:
Switch# configure terminal
Switch(config)# overlay
Switch(config-overlay)# no source

Related Commands

None
17.1.6 remote-vtep

Command Purpose
Use the overlay remote vtep command to specify the peer ip address and type of overlay entry. Use the no form of this command to remove the peer ip address and type of overlay entry.

Command Syntax
remote-vtep INDEX ip-address IP_ADDR_VTEP type ( vxlan | nvgre | geneve ) ( { src-ip IP_ADDR | split-horizon-disable | keep-vlan-tag } | )
no remote-vtep index

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INDEX</td>
<td>Remote vtep index</td>
<td>1-65535</td>
</tr>
<tr>
<td>vxlan-peer</td>
<td>Remote vtep is vxlan vtep</td>
<td>-</td>
</tr>
<tr>
<td>nvgre-peer</td>
<td>Remote vtep is nvgre vtep</td>
<td>-</td>
</tr>
<tr>
<td>geneve-peer</td>
<td>Remote vtep is geneve vtep</td>
<td>-</td>
</tr>
<tr>
<td>IP_ADDR_VTEP</td>
<td>The overlay peer ip address, it should be a valid interface ip address.</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>Specify the overlay source ip address, it should be a valid interface ip address, it would use the global source ip address in default</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>horizon-split-disable</td>
<td>Support to close horizon split of the tunnel with this vtep</td>
<td>-</td>
</tr>
<tr>
<td>keep-vlan-tag</td>
<td>means the vlan tags of original packet will not be stripped</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
OVERLAY Configuration

Default
None

Usage
This command is used to specify overlay vtep peer address and type on remote device, administrator must know all the peer addresses and types on the Data Center network and make sure that they can route between each other.

Examples
The following example sets the overlay vxlan vtep peer address 2.2.2.2 with source ip address 1.1.1.1:
```
Switch# configure terminal
Switch(config)# overlay
Switch(config-overlay)# remote-vtep 20 ip-address 2.2.2.2 type vxlan src-ip 1.1.1.1
```
The following example removes remote vtep:
```
Switch# configure terminal
Switch(config)# overlay
Switch(config-overlay)# no remote-vtep 20
```

Related Commands
None
17.1.7 dscp-strategy

**Command Purpose**
Use the overlay remote vtep command to configure the outer ip dscp gaining mode.

**Command Syntax**
remote-vtep INDEX encapsulation-dscp-strategy { dscp-copy | priority-map | custom-assign VALUE }

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INDEX</td>
<td>Remote vtep index</td>
<td>1-65535</td>
</tr>
<tr>
<td>dscp-copy</td>
<td>Copy from inner ip dscp</td>
<td></td>
</tr>
<tr>
<td>priority-map</td>
<td>Map from priority of qos</td>
<td></td>
</tr>
<tr>
<td>custom-assign</td>
<td>Assign dscp by users</td>
<td>0-63</td>
</tr>
</tbody>
</table>

**Command Mode**
OVERLAY Configuration

**Default**
Dscp-copy

**Usage**
When dscp-strategy is set priority-map, please configure QOS priority by MQC.

**Examples**
The following example sets overlay dscp-strategy as custom-assign:
```
Switch# configure terminal
Switch(config)# overlay
Switch(config-overlay)# remote-vtep 20 dscp-strategy custom-assign 63
remote-vtep
```

**Related Commands**
None

17.1.8 Virtual-mac

**Command Purpose**
Use the overlay virtual mac command to specify the virtual route mac address of remote vtep. Use the no form of this command to remove the virtual mac address of remote vtep.

**Command Syntax**
remote-vtep INDEX virtual-mac MAC
no remote-vtep index virtual-mac
### Command Mode

**OVERLAY Configuration**

**Default**

None

**Usage**

The virtual mac address will be used as the inner mac address of DVR routes which don't specify the inner mac address.

**Examples**

The following example sets the overlay remote vtep with the virtual mac a.a.a:

Switch# configure terminal
Switch(config)# overlay
Switch(config-overlay)# remote-vtep virtual-mac a.a.a

The following example removes remote vtep virtual mac address:

Switch# configure terminal
Switch(config)# overlay
Switch(config-overlay)# no remote-vtep virtual-mac a.a.a

**Related Commands**

None

17.1.9  **vlan remote-vtep**

**Command Purpose**

Use the overlay peer command to specify the peer ip address and type of overlay vlan entry. Use the no form of this command to remove the peer ip address and type of overlay vlan entry.

**Command Syntax**

`vlan VLAN_ID remote-vtep INDEX ( tunnel-aware inner | )`

`no vlan VLAN_ID remote-vtep INDEX`
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan id</td>
<td>2-4094</td>
</tr>
<tr>
<td>INDEX</td>
<td>The overlay remote vtep index</td>
<td>1-65535</td>
</tr>
<tr>
<td>inner</td>
<td>If set, ACL/Flow tracing will use inner packet header information</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**

OVERLAY Configuration

**Default**

None

**Usage**

Make sure the remote vtep is already created when setting vlan with remote vtep index.

**Examples**

The following example sets the overlay vlan 20 with remote vtep 2:

```
Switch# configure terminal
Switch(config)# overlay
Switch(config-overlay)# vlan 20 remote-vtep 2
```

The following example removes remote vtep 3 from vlan 20:

```
Switch# configure terminal
Switch(config)# overlay
Switch(config-overlay)# no vlan 20 remote-vtep 3
```

**Related Commands**

None

**17.1.10 overlay uplink**

**Command Purpose**

Use the overlay uplink command to enable or disable overlay uplink port capability.

**Command Syntax**

```
overlay uplink { enable | disable }
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Make overlay uplink port enable</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>Make overlay uplink port disable</td>
<td>-</td>
</tr>
</tbody>
</table>
Command Mode

Interface Configuration

Default

Disable

Usage

The command is allow setting on ether type port. When the port is routed port or routed link agg port, it can work both on normal ecmp mode and advanced ecmp mode. When the port belongs to vlan interface, it can only work on normal ecmp mode.

Examples

This example shows how to enable overlay uplink on interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# overlay uplink enable
```

This example shows how to disable overlay uplink on interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# overlay uplink disable
```

Related Commands

None

17.1.11  mac-address-table forward remote-vtep

Command Purpose

Use the overlay static fdb command to add or delete overlay static fdb.

Command Syntax

```
mac-address-table MAC_ADDR forward remote-vtep INDEX vlan VLAN_ID
```

```
no mac-address-table mac-addr forward remote-vtep index vlan VLAN_ID
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC_ADDR</td>
<td>Destination MAC addresses (unicast) to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface</td>
<td>MAC Address</td>
</tr>
<tr>
<td>INDEX</td>
<td>The index of remote vtep</td>
<td>1-65535</td>
</tr>
<tr>
<td>VLAN_ID</td>
<td>Specify the VLAN for which the packet with the specified MAC address is received.</td>
<td>2-4094</td>
</tr>
</tbody>
</table>
**Command Mode**
Global Configuration

**Default**
None

**Usage**
None

**Examples**
This example shows how to add a static overlay FDB with remote-vtep 3 and vlan 2:
Switch# configure terminal
Switch(config)# mac-address-table 1.1.1 forward remote-vtep 3 vlan 2
This example shows how to delete a static overlay FDB with remote-vtep 3 and vlan 2:
Switch# configure terminal
Switch(config)# no mac-address-table 1.1.1 forward remote-vtep 3 vlan 2

**Related Commands**
None

**17.1.12 overlay gateway**

**Command Purpose**
Use the overlay dvrf enable command to enable or disable advanced function for overlay gateway.

**Command Syntax**

overlay gateway { enable | disable }

**Command Mode**

VRF Configuration

Global Configuration

**Default**

Disable

**Usage**
This command will let the central gateway do routing, when there is none local dvrf route entry. The command in Global Configuration is for default vrf

**Examples**
This example shows how to enable overlay gateway advanced function on default vrf:
Switch# configure terminal
Switch(config)# ip vrf tenant1
Switch(config-vrf)# overlay gateway enable
This example shows how to disable overlay dvrf on vrf:
Switch# configure terminal
Switch(config)# ip vrf tenant1
Switch(config-vrf)# overlay gateway disable
Related Commands
None

17.1.13 gateway-mac

Command Purpose
Use the overlay gateway command to add or delete overlay gateway mac address.

Command Syntax

```
vlan VLAN_ID gateway-mac mac-addr
no vlan VLAN_ID gateway-mac mac-addr
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan id</td>
<td>2-4094</td>
</tr>
<tr>
<td>mac-addr</td>
<td>Gateway MAC addresses (unicast) which VMs will use when they need</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>to do routing.</td>
<td></td>
</tr>
</tbody>
</table>

Command Mode

OVERLAY Configuration

Default
None

Usage
The downlink port should be in trunk mode.

Examples

This example shows how to add an overlay gateway with vlan 2:
```
Switch# configure terminal
Switch(config)# overlay
Switch(config-overlay)# vlan 2 gateway-mac 2.2.2
```

This example shows how to delete an static overlay fdb with nvgre vtep peer 2.2.2.2 and vlan 2:
```
Switch# configure terminal
Switch(config)# overlay
Switch(config-overlay)# no vlan 2 gateway-mac 2.2.2
```

Related Commands
None
17.1.14 ip route remote-vtep

Command Purpose

Use the overlay route command to add or delete overlay static routes.

Command Syntax

ip route vrf VRF_NAME (ADDRESS WILDCARD-MASK | ADDRESS/PREFIX-LENGTH) remote-vtep INDEX vni VNI ( | inner-macda mac-addr )

no ip route vrf VRF_NAME (ADDRESS WILDCARD-MASK | ADDRESS/PREFIX-LENGTH) remote-vtep INDEX vni VNI ( | inner-macda mac-addr )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF_NAME</td>
<td>Vrf name</td>
<td>Up to 15 characters</td>
</tr>
<tr>
<td>ADDRESS</td>
<td>IPv4 address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>WILDCARD-MASK</td>
<td>Mask for the associated IP subnet</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PREFIX-LENGTH</td>
<td>Prefix length of the address</td>
<td>1-32</td>
</tr>
<tr>
<td>INDEX</td>
<td>The index of remote vtep</td>
<td>1-65535</td>
</tr>
<tr>
<td>VNI</td>
<td>vni id</td>
<td>1-16777215</td>
</tr>
<tr>
<td>MAC_ADDR</td>
<td>Inner mac destination address</td>
<td>MAC Address</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

None

Usage

If the inner mac destination address is not specified, it will use the remote vtep's virtual mac address as the inner mac destination address.

Examples

This example shows how to add an overlay route:

Switch# configure terminal
Switch(config)# ip route vrf tenant1 3.3.3.3/32 remote-vtep 3 vni 50000 inner-macda a.a.a
Switch(config)# ip route vrf tenant1 4.4.4.4/32 remote-vtep 3 vni 50000

This example shows how to delete an overlay route:

Switch# configure terminal
Switch(config)# no ip route vrf tenant1 3.3.3.3/32 nvgre-peer 5.5.5.5 vni 50000 inner-macda a.a.a
Switch(config)# no ip route vrf tenant1 4.4.4.4/32 nvgre-peer 5.5.5.5 vni 50000

Related Commands

None
17.1.15 overlay distributed-gateway

Command Purpose
Use the command to enable or disable overlay distributed gateway.

Command Syntax
overlay distributed-gateway ( enable | disable )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enable overlay distributed gateway</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>Disable overlay distributed gateway</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
None

Usage
None

Examples
This example shows how to enable overlay distributed gateway:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# overlay distributed-gateway enable

Related Commands
None

17.1.16 vxlan udp-dest-port

Command Purpose
Use the command to config vxlan udp destport value.

Command Syntax
vxlan udp-dest-port PORT
no vxlan udp-dest-port

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PORT</td>
<td>udp destport value</td>
<td>1024-65535</td>
</tr>
</tbody>
</table>

Command Mode
OVERLAY Configuration
Default
4789

Usage
When use this function, should make two switch config the same value

Examples
This example shows how to config vxlan udp destport value:
Switch# configure terminal
Switch(config)# overlay
Switch(config-overlay)# vxlan udp-dest-port 8888

Related Commands
17.1.17 qos tunnel-aware inner

Command Purpose
Use inner packet information to process packet (eg ACL, Flow tracing processing). This command is used for overlay packets without tunnel decapsulation processing.

Command Syntax
(no | ) qos tunnel-aware inner

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disable inner parse</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
Disable

Usage
This command is used to force inner packet header process for overlay packets without tunnel decapsulation.

Examples
This example shows how to enable force inner parse on interface:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# qos tunnel-aware inner

Related Commands
None
17.1.18  qos tunnel-aware inner-outer-merge

**Command Purpose**
Use inner and outer packet information to process packet (eg ACL, Flow tracing processing).

**Command Syntax**
( no | ) inner-outer merge enable

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disable inner-outer merge mode</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**
Interface Configuration

**Default**
Disable

**Usage**
This command is used to force inner and packet header information process for overlay packets.

**Examples**
This example shows how to enable inner and outer parse on interface:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# qos tunnel-aware inner-outer-merge

**Related Commands**
None

17.1.19  Show overlay

**Command Purpose**
Use the show overlay command to show related overlay information.

**Command Syntax**
show overlay ( vlan VLAN_ID )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_ID</td>
<td>Vlan id</td>
<td>2-4094</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC

**Default**
None
Usage

None

Examples

This example shows all the overlay information:

Switch# show overlay

```
-------------------------------------------------------------------
ECMP Mode : Normal
Source VTEP : 20.1.1.1
Vlan Vni Type Remote-vtep IP-Address Src-Address Split-Horizon
-------------------------------------------------------------------
10 10000 VxLAN 1 2.2.2.2 1.1.1.1 Enable
-------------------------------------------------------------------
```

This example shows the overlay information of vlan 2:

Switch# show overlay vlan 2

```
-------------------------------------------------------------------
ECMP Mode : Normal
Source VTEP : 1.1.1.1
Remote VTEP Index: 1, Ip address: 2.2.2.2, Type: VxLAN
Remote VTEP Index: 2, Ip address: 3.3.3.3, Type: VxLAN
-------------------------------------------------------------------
VLAN ID : 2
VNI : 20000
Remote VTEP NUM: 2
    Index: 1, Ip address: 2.2.2.2, Type: VxLAN
    Index: 2, Ip address: 3.3.3.3, Type: VxLAN
DVR Gateway NUM: 0
-------------------------------------------------------------------
```

Related Commands

None

17.2 PFC Commands

17.2.1 priority-flow-control mode

Command Purpose
Use this command to enable or disable priority-based flow control function on the interface.

Command Syntax

```
priority-flow-control mode ( on | auto )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>enable priority-based flowcontrol no matter how the peer configures</td>
<td>-</td>
</tr>
<tr>
<td>auto</td>
<td>enable priority-based flowcontrol negotiating with the peer</td>
<td>-</td>
</tr>
</tbody>
</table>
**Command Mode**

Interface Configuration

**Default**

Enable priority-based flowcontrol on priority 3

**Usage**

Use the priority-flow-control interface Configuration command to set the interface's ability to send pause frames to on or off on the specified priorities.

**Examples**

This example shows how to enable priority-based flowcontrol on the interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# priority-flow-control mode on
```

This example shows how to enable priority-based flowcontrol on the interface(auto negotiating with the peer):

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# priority-flow-control mode auto
```

**Related Commands**

None

17.2.2 priority-flow-control enable priority

**Command Purpose**

Use this command to enable or disable priority-based flow control function on which priority.

**Command Syntax**

```
priority-flow-control enable priority <0-7> ( <0-7> ( <0-7> ( <0-7> ( <0-7> ( <0-7> ( <0-7> ( <0-7> | ) ) ) ) ) ) ) ) )
nopriority-flow-control enable priority <0-7> ( <0-7> ( <0-7> ( <0-7> ( <0-7> ( <0-7> ( <0-7> ( <0-7> | ) ) ) ) ) ) ) ) )
```

**Command Mode**

Interface Configuration

**Default**

Enable priority-based flowcontrol on priority 3

**Usage**

Use the priority-flow-control enable priority interface Configuration command to set the interface's ability to send pause frames to on or off on which priorities.

**Examples**

This example shows how to enable priority-based flowcontrol on which priorities:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# priority-flow-control enable priority 1 3 4 7
```
Related Commands
None

17.2.3 show priority-flow-control

Command Purpose
Use this command to display priority-based flowcontrol information.

Command Syntax
show priority-flow-control (interface IFNAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical ports</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
Use the command to display priority-based flowcontrol admin-config and operation-config information of each port.

Examples
This example shows how to display priority-based flowcontrol information:
Switch# show priority-flow-control interface eth-0-1

Related Commands
None

17.2.4 show priority-flow-control statistics

Command Purpose
Use this command to display the statistic of priority-based flowcontrol.

Command Syntax
show priority-flow-control statistics ( IFNAME | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
<td>Support physical ports</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None
Usage
Use the command to display the counting information of pause frames for priority-based flowcontrol.

Examples
This example shows how to display the counting information of pause frames for priority-based flowcontrol:
Switch# show priority-flow-control statistics interface eth-0-1

Related Commands
None

17.3 EFD Commands

17.3.1 efd enable

Command Purpose
Use this command to enable EFD detect on interface. Use the no form of this command to disable EFD detect on interface.

Command Syntax
efd enable
no efd enable

Command Mode
Interface Configuration

Default
EFD detect is disabled

Usage
When the rate of the flow is 60Mbps, this flow shall be a elephant flow.

Examples
This example shows how to enable EFD on the interface:
Switch# configure terminal
Switch(config-if)# efd enable

Related Commands
None

17.3.2 efd tcp-only enable

Command Purpose
Use this command to enable detect EFD with TCP packet. Use the no form of this command to disable detect EFD with TCP.
**Command Syntax**

`efd tcp-only enable`

`no efd tcp-only enable`

**Command Mode**

Global Configuration

**Default**

All flow will be detect

**Usage**

None

**Examples**

This example shows how to enable EFD on the interface:

```
Switch# configure terminal
Switch(config)# efd tcp-only enable
```

**Related Commands**

None

### 17.3.3 `efd flow-traffic-class`

**Command Purpose**

Use this command to set traffic class for flow detected as EFD. Use the no form of this command to unset traffic class for flow detected as EFD.

**Command Syntax**

`efd flow-traffic-class CLASS`

`no efd flow-traffic-class`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLASS</td>
<td>Traffic class value</td>
<td>0-6</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

Disabled

**Usage**

None
Examples
This example shows how to set flow-traffic-class as 5 for EFD flow:
Switch# configure terminal
Switch(config)# efd flow-traffic-class 5

Related Commands
None

17.3.4 efd flow-color

Command Purpose
Use this command to set flow color for flow detected as EFD. Use the no form of this command to unset flow color for flow detected as EFD.

Command Syntax
efd flow-color ( green | red | yellow )
no efd flow-color

Parameter | Parameter Description | Parameter Value
---|---|---
green | Let the flow be tinged with green | -
red | Let the flow be tinged with red | -
yellow | Let the flow be tinged with yellow | -

Command Mode
Global Configuration

Default
Disabled

Usage
None

Examples
This example shows how to set flow color as yellow for EFD flow:
Switch# configure terminal
Switch(config)# efd flow-color yellow

Related Commands
None
17.3.5  efd detect speed

**Command Purpose**
Use this command to set speed for flow detected as EFD.

**Command Syntax**
efd detect speed SPEED
efd detect speed

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPEED</td>
<td>Detect speed, Mbps.</td>
<td>1-10000</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
50Mbps

**Usage**
None

**Examples**
This example shows how to set 60Mbps detect for EFD flow:
```
Switch# configure terminal
Switch(config)# efd detect speed 60
```

**Related Commands**
None

17.3.6  efd detect granularity

**Command Purpose**
Use this command to set the granularity of calculate the detect rate. The greater the granularity, the greater the quantized error.

**Command Syntax**
efd detect granularity (4B | 8B | 16B | 32B)
efd detect granularity

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>4B</td>
<td>8B</td>
<td>16B</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
16B
Usage
(Rate * Interval) >> Granularity, the value's bit is fixed.

Examples
This example shows how to set 32B granularity:
Switch# configure terminal
Switch(config)# efd detect granularity 32B

Related Commands
None

17.3.7 efd detect time-interval

Command Purpose
Use this command to set the time interval for flow as detected as EFDs.

Command Syntax
efd detect time-interval INTERVAL

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>Time interval in ms(10ms - 100000ms, default value is 30ms)</td>
<td>10-100000</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
30ms

Usage
None

Examples
This example shows how to set time interval to 100ms:
Switch# configure terminal
Switch(config)# efd detect time-interval 100

Related Commands
None

17.3.8 efd detect min-pkt-size

Command Purpose
Use this command to set flow color for flow detected as EFD. Use the no form of this command to unset flow color for flow detected as EFD.
Command Syntax

efd detect min-pkt-size SIZE

no efd detect min-pkt-size

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIZE</td>
<td>Configure minimum packet size, unit is byte</td>
<td>64-9216</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

Disabled

Usage

unit is byte.

Examples

This example shows how to set elephant flow minimum packet size with 300:

Switch# configure terminal
Switch(config)# efd detect min-pkt-size 300

Related Commands

show efd configuration

17.3.9 efd aging-period

Command Purpose

Use this command to set flows detected as EFDs aging period.

Command Syntax

efd aging-period PERIOD

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERIOD</td>
<td>Aging period, configure 2 ~ 7 times of configured detect time-interval, default value is 4</td>
<td>2-7</td>
</tr>
</tbody>
</table>

Command Mode

Global Configuration

Default

4

Usage

The aging time is the detect rate multiple aging period.
Examples
This example shows how to set aging period to 3:
Switch# configure terminal
Switch(config)# efd aging-period 3

Related Commands
None

17.3.10 efd redirect to interface

Command Purpose
Use this command to redirect the flows detected as EFD to the specified interface.

Command Syntax
efd redirect to interface IFNAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>The interface to redirect to</td>
<td>Support physical/aggregation ports</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
Disable

Usage
None

Examples
This example shows how to redirect the flows to interface eth-0-2:
Switch# configure terminal
Switch(config)# efd redirect to interface eth-0-2

Related Commands
None

17.3.11 efd ipg enable

Command Purpose
Use this command to set calculate the detect rate whether use the packet's ipg.Use the no form of this command to unset calculate the detect rate whether use the packet's ipg.

Command Syntax
efd ipg enable
no efd ipg enable
**Command Mode**
Global Configuration

**Default**
Disable

**Usage**
None

**Examples**
This example shows how to enable the calculate the detect rate with ipg:

```
Switch# configure terminal
Switch(config)# efd ipg enable
```

**Related Commands**
None

**17.3.12 efd notify enable**

**Command Purpose**
Use this command to configure EFD notify function. Use the no form of this command to unconfigure EFD notify function.

**Command Syntax**
```
efd notify enable IP_ADDR ( PORT )
```

```
no efd notify enable
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>IP address of the server</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>PORT</td>
<td>UDP port used by server</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
The feature is disabled.
The default UDP port is 20007 if not specified.

**Usage**
After EFD notify enabled, the new elephant flow will be notified to server, the format of the data in the UDP packet is:

```
<table>
<thead>
<tr>
<th>---rsv---</th>
<th>ver</th>
<th>code</th>
</tr>
</thead>
<tbody>
<tr>
<td>---type--</td>
<td>----</td>
<td>len--</td>
</tr>
<tr>
<td>------- value-------</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

......
Examples

This example shows how to configure EFD notify:
Switch# configure terminal
Switch(config)# efd notify enable 10.10.10.1

Related Commands
efd enable
efd notify packet

17.3.13 efd notify packet

Command Purpose
Use this command to configure EFD notify carry original packet. Use the no form of this command to unconfigure EFD notify carry original packet.

Command Syntax
efd notify packet
no efd notify packet

Command Mode
Global Configuration

Default
Disabled

Usage
None

Examples
This example shows how to configure EFD notify carry original packet:
Switch# configure terminal
Switch(config)# efd notify packet

Related Commands
efd enable
efd notify enable

17.3.14 efd black-hole-route gw

Command Purpose
Use this command to enable EFD black hole route, specify the gateway address and route tag. Use the no form of this command to disable EFD black hole route, unspecify the gateway address and route tag.
**efd black-hole-route gw IP_ADDR ( | tag TAG_VALUE )**

Command Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>Gateway address of black hole route</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>TAG_VALUE</td>
<td>Tag of black hole route</td>
<td>0-4294967295</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

None

**Usage**

Enable EFD black hole route feature, a black hole route would be created for it when a flow is detected as elephant flow, it’s next-hop would be pointed to the configured gateway address.

**Examples**

This example shows how to enable efd black hole route:

Switch# efd black-hole-route gw 1.2.3.4 tag 876

**Related Commands**

tool efd bhr information detail

**efd black-hole-route aging-timer**

**Command Purpose**

Use this command to set black hole route aging time. Use the no form to this command to unset black hole route aging time.

**Command Syntax**

efd black-hole-route aging-timer ( 0 | value )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Never aging</td>
<td>-</td>
</tr>
<tr>
<td>VALUE</td>
<td>The black hole route aging time</td>
<td>10-1000000 seconds</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration
Default
300

Usage
None

Examples
This example shows how to set aging time:
Switch# efd black-hole-route aging-timer 1000

Related Commands
None

17.3.16 efd syslog enable

Command Purpose
Use this command to set the efd detect information. Use the no form of this command to unset the efd detect information.

Command Syntax
efd syslog enable
no efd syslog enable

Command Mode
Global Configuration

Default
Enable

Usage
None

Examples
This example shows how to set the efd detect information:
Switch# efd syslog enable

Related Commands
None

17.3.17 show efd bhr information

Command Purpose
Use this command to display the information about efd black hole route.

Command Syntax
show efd bhr information (detail | )
Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to display the information about efd black hole route:
Switch# show efd bhr information detail

Elephant flow detection BHR configuration information:
* BHR - Black Hole Route
--------------------------------------------------
Auto install BHR : Enabled
BHR gateway : 1.2.3.4
BHR count : 1
BHR aging timer : 300
BHR route tag : 876

--------------------------------------
BHR Prefix, Age Time :
--------------------------------------
  12.12.12.2/32, 1 min

Related Commands
efd black-hole-route gw
efd black-hole-route aging-timer

17.3.18  show efd configuration

Command Purpose
Use this command to display the configuration of efd.

Command Syntax
show efd configuration

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to display the configuration of efd:
Switch# show efd configuration

Elephant flow detection configuration information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect rate</td>
<td>50 Mbps</td>
</tr>
<tr>
<td>Detect granularity</td>
<td>16B</td>
</tr>
<tr>
<td>Detect time interval</td>
<td>30 ms</td>
</tr>
<tr>
<td>Black-hole-route gateway</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Black-hole-route tag</td>
<td>0</td>
</tr>
<tr>
<td>Black-hole-route aging time</td>
<td>0</td>
</tr>
<tr>
<td>EFD syslog</td>
<td>Enable</td>
</tr>
<tr>
<td>EFD aging period</td>
<td>4 times</td>
</tr>
<tr>
<td>EFD aging time</td>
<td>120 ms – 150 ms</td>
</tr>
<tr>
<td>EFD detect packet type</td>
<td>All IP packets</td>
</tr>
<tr>
<td>EFD IPG</td>
<td>disable</td>
</tr>
<tr>
<td>EFD redirect interface</td>
<td>N/A</td>
</tr>
<tr>
<td>EFD flow-traffic-class</td>
<td>N/A</td>
</tr>
<tr>
<td>EFD flow-color</td>
<td>N/A</td>
</tr>
<tr>
<td>EFD notify</td>
<td>1.2.3.4 20007</td>
</tr>
<tr>
<td>EFD notify packet</td>
<td>disable</td>
</tr>
<tr>
<td>EFD min-pkt-size</td>
<td>disable</td>
</tr>
<tr>
<td>EFD flow hash fields</td>
<td>source-ip</td>
</tr>
<tr>
<td></td>
<td>destination-ip</td>
</tr>
<tr>
<td></td>
<td>ip-protocol</td>
</tr>
<tr>
<td></td>
<td>layer4-source-port</td>
</tr>
<tr>
<td></td>
<td>layer4-destination-port</td>
</tr>
<tr>
<td>EFD enabled interface</td>
<td>eth-0-1, eth-0-9, eth-0-10, agg5</td>
</tr>
</tbody>
</table>

Related Commands

None

17.3.19 show efd flow table

Command Purpose

Use this command to display the efd flow hardware information.

Command Syntax

show efd flow table

Command Mode

Privileged EXEC

Default

None

Usage

None
Examples

This example shows how to display the efd flow hardware information:

Switch# show efd flow table

Current elephant flow number is 0, valid bit count is 0
Flow Entry Status: 'V' --- Valid, '.' --- Not Valid
FlowId --------------------------
(00)0000~0031 ......................
(01)0032~0063 ......................
(02)0064~0095 ......................
(03)0096~0127 ......................
(04)0128~0159 ......................
(05)0160~0191 ......................
(06)0192~0223 ......................

Related Commands

None

17.3.20 show efd flow information

Command Purpose
Use this command to display EFD flow information.

Command Syntax
show efd flow information

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
This example shows how to display EFD flow information:
Switch# show efd flow information

Related Commands
None

17.3.21 clear efd flow information

Command Purpose
Use this command to clear EFD flow information.
**Command Syntax**

*clear efd flow information*

**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

This example shows how to clear EFD flow information:

```
Switch# clear efd flow information
```

**Related Commands**

None

---

**17.4 Flow hash Commands**

**17.4.1 flow hash-field-select**

**Command Purpose**

Use this command to enable or disable priority-based flow control function on the interface. Use this command to calculate packet's hash value, this hash value is used to identify the packet. Flow hash value is used by EFD to select flow entry from EFD flow table. Flow hash value is also used by ECMP to select flow entry from ECMP flow table.

**Command Syntax**

```
flow hash-field-select { ipda | ipsa | ip-protocol | sourceport | destport | vxlan-vni | nvgre-vsid | inner-ipda | inner-ipsa | inner-ip-protocol | inner-sourceport | inner-destport }
```

```
no flow hash-field-select
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipda</td>
<td>IP Destination Address</td>
<td>-</td>
</tr>
<tr>
<td>ipsa</td>
<td>IP Source Address</td>
<td>-</td>
</tr>
<tr>
<td>ip-protocol</td>
<td>IP Header protocol</td>
<td>-</td>
</tr>
<tr>
<td>sourceport</td>
<td>Layer4 Source Port</td>
<td>-</td>
</tr>
<tr>
<td>destport</td>
<td>Layer4 Destination Port</td>
<td>-</td>
</tr>
<tr>
<td>vxlan-vni</td>
<td>VXLAN VNI</td>
<td>-</td>
</tr>
<tr>
<td>nvgre-vsid</td>
<td>NVGRE VSID</td>
<td>-</td>
</tr>
<tr>
<td>inner-ipda</td>
<td>Inner header's IP Source Address</td>
<td>-</td>
</tr>
<tr>
<td>inner-ipsa</td>
<td>Inner header's IP Destination Address</td>
<td>-</td>
</tr>
<tr>
<td>inner-ip-protocol</td>
<td>Inner header's IP Header protocol</td>
<td>-</td>
</tr>
<tr>
<td>inner-sourceport</td>
<td>Inner header's Layer4 Source Port</td>
<td>-</td>
</tr>
<tr>
<td>inner-destport</td>
<td>Inner header's Layer4 Destination Port</td>
<td>-</td>
</tr>
</tbody>
</table>
**Command Mode**
Global Configuration

**Default**
Use ipda, ipsa, ip-protocol, sourceport and destport

**Usage**
Use this command to generate flow hash value to identify the packet/flow, and this flow hash value is used to select EFD entry from EFD flow table. This flow hash value is also used to select ECMP entry from ECMP flow table in dynamic ECMP.

**Examples**
This example shows how to select ipsa and ipsa for hash filed calculate:
```
Switch# configure terminal
Switch(config)# flow hash-field-select ipda ipsa
```

**Related Commands**
None

### 17.5 OVSDB Commands

#### 17.5.1 ovsdb enable

**Command Purpose**
Use this command to set ovsdb enable/disable.

**Command Syntax**
```
ovsdb enable {management-ip IP_ADDR | none-mgmt-if }
```
```
no ovsdb enable
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>Configure the management IP address, it will be set to VTEP database</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>none-mgmt-if</td>
<td>Configure the client connect to OVSDB server from in-band interface</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
Disable

**Usage**
All overlay configurations will be controlled by OVSDB after OVSDB function enabled in switch. The passive TCP connection will be open with port 6632 when ovsdb enabling.
**Examples**
The following example shows how to enable OVSDB:
```
Switch# configure terminal
Switch(config)# ovsdb enable management-ip 192.168.1.1
```

**Related Commands**
`ovsdb port enable`

### 17.5.2 ovsdb port enable

**Command Purpose**
Use this command to let the port controlled by OVSDB. To restore the default value, use the no form of this command.

**Command Syntax**
```
ovsdb port enable

no ovsdb port enable
```

**Command Mode**
Interface Configuration

**Default**
None

**Usage**
There are no overlay configurations specified by OVSDB if none port is controlled by OVSDB

**Examples**
The following example shows how to enable OVSDB on port:
```
Switch# configure terminal
Switch(config-if)# ovsdb port enable
```

**Related Commands**
`ovsdb enable`

### 17.5.3 ovsdb virtual-port

**Command Purpose**
Use this command to configure the virtual port like tunnel controlled by OVSDB. To unset the configuration, use the no form of this command.

**Command Syntax**
```
ovsdb virtual-port NAME

no ovsdb virtual-port
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>The name of virtual port</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration

**Default**

None

**Usage**

None

**Examples**

The following example shows how to configure the virtual port:

```
Switch# configure terminal
Switch(config)# ovsdb virtual-port tunnel1
```

**Related Commands**

**17.5.4 ovsdb controller**

**Command Purpose**

Use this command to configure IP address of OVSDB controller. To restore the default value, use the no form of this command.

**Command Syntax**

```
ovsdb controller IP_ADDR ( port NUM )
```

no ovsdb controller

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>Specify IP address of OVSDB controller</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>NUM</td>
<td>Specify the port for TCP connection</td>
<td>1-65535</td>
</tr>
</tbody>
</table>

**Command Mode**

Global Configuration
Default

There is none controller by default.

The default TCP port is 6632 if not specified.

Usage

The default TCP port for connection is 6632.

Examples

The following example shows how to configure the IP address of controller:

```
Switch# configure terminal
Switch(config)# ovsdb controller 192.168.1.2
```

Related Commands

ovsdb enable

17.5.5 debug ovsdb

Command Purpose

Use this command to configure the level of OVSDB log to display. To restore the default value, use the no form of this command.

Command Syntax

```
ddebug ovsdb { server | agent } { event | level } { error | warning | information | debug }
nno debug ovsdb { server | agent } { level | event }
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Configure level for OVSDB server</td>
<td>-</td>
</tr>
<tr>
<td>agent</td>
<td>Configure level for OVSDB agent</td>
<td>-</td>
</tr>
<tr>
<td>event</td>
<td>Configure event for OVSDB agent and server</td>
<td>-</td>
</tr>
<tr>
<td>error</td>
<td>The level of log to display is ERROR</td>
<td>-</td>
</tr>
<tr>
<td>warning</td>
<td>The level of log to display is WARNING</td>
<td>-</td>
</tr>
<tr>
<td>information</td>
<td>The level of log to display is INFORMATION</td>
<td>-</td>
</tr>
<tr>
<td>debug</td>
<td>The level of log to display is DEBUG</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC
Default

None

Usage

For the configuration take effect, this command should be input after OVSDB enabled on switch.

Examples

The following example shows how to modify the level of OVSDB log to display:

```
Switch# debug ovsdb server level debug
```

Related Commands

ovsdb enable

17.5.6 show ovsdb

Command Purpose

Use this command to display the information in VTEP database.

Command Syntax

```
show ovsdb ( physical-switch ( port | binding IFNAME ) | logical-switch | remote-macs ( LSNAME ) )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>physical-switch</td>
<td>Display the information of physical switch in VTEP database</td>
<td>-</td>
</tr>
<tr>
<td>port</td>
<td>Display the information of physical port in VTEP database</td>
<td>-</td>
</tr>
<tr>
<td>binding IFNAME</td>
<td>Display the bindings of specified port in VTEP database</td>
<td>Aggregation and physical interface</td>
</tr>
<tr>
<td>logical-switch</td>
<td>Display the information of logical switch in VTEP database</td>
<td>-</td>
</tr>
<tr>
<td>remote-macs (LSNAME)</td>
<td>Display the remote MACs of specified logical switch in VTEP database</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None
Usage

None

Examples

The following example shows how to display the physical switch in VTEP database:

Switch# show ovsdb physical-switch

<table>
<thead>
<tr>
<th>Physical Switch Name</th>
<th>Management IP address</th>
<th>Tunnel IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>switchA4D92AFF400</td>
<td></td>
<td>2.2.2.1</td>
</tr>
</tbody>
</table>

Related Commands

ovsdb enable

17.6  EVVPN Commands

17.6.1  address-family l2vpn evpn

Command Purpose

Use this command to enter EVVPN address family configure mode.

Use the no parameter of this command to cancel EVVPN configuration in BGP.

Command Syntax

address-family l2vpn evpn
no address-family l2vpn evpn

Command Mode

Router Configuration

Default

None

Usage

Use the address family command to enter the address family mode allowing configuration of address-family specific parameters. To leave the address family mode and return to the Configure mode use the exit-address-family command.

EVPN feature should be enabled before enter this address family configure mode.
Examples

The following example shows how to EVPN address family configure mode:

```
Switch# configure terminal
Switch(config)# router bgp 1
Switch(config-router)# address-family l2vpn evpn
Switch(config-router-af)#
```

Related Commands

`exit-address-family`

17.6.2 debug overlay evpn

Command Purpose

Use this command to enable all EVPN troubleshooting functions on Overlay.
Use no format of this command to disable this configuration.

Command Syntax

```
debug overlay evpn
no debug overlay evpn
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to debug EVPN on overlay:
```
Switch# debug overlay evpn
```

Related Commands

`overlay host-collect`
17.6.3 evpn

Command Purpose

Use this command to enable EVPN function and enter EVPN configure mode.
Use no format of this command to disable EVPN function.

Command Syntax

evpn
devn

Command Mode

Global Configuration

Default

Disable

Usage

This command can enable EVPN function. And after entering EVPN configure mode, EVPN instance can be created. When the function had been disabled, all EVPN instances will be deleted.

Examples

The following example shows how to enable EVPN function:
Switch# configure terminal
Switch(config)# evpn
Switch(config-evpn)#

Related Commands

address-family l2vpn evpn

17.6.4 overlay host-collect

Command Purpose

Use this command to enable host information collection.
Use no format of the command to disable this configuration.
Command Syntax

overlay host-collect ( enable | disable )

Command Mode

Interface Configuration

Default

Disable

Usage

After host collection was enabled and both RD and route-target of EVPN instance was configured, host information from dynamic arp will be sent to BGP module to format and advertise EVPN type 2 route.

Examples

The following example shows how to enable host information collection on interface:

Switch# configure terminal
Switch(config)# interface vlan 100
Switch(config-if)# overlay host-collect enable

Related Commands

Evpn

17.6.5 Rd

Command Purpose

Use this command to set route distinguisher for EVPN instance.

Command Syntax

rd ( auto | RD-VALUE )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Automatically generates an RD in the N:VXLAN ID format</td>
<td>-</td>
</tr>
<tr>
<td>RD-VALUE</td>
<td>Route distinguisher value. ASN:nn or IP:nn</td>
<td>ASN range is 1-4294967295 nn range is 1-65535</td>
</tr>
</tbody>
</table>

Command Mode

EVI Configuration
Default

None

Usage

None

Examples

The following example shows how to set rd:

```
Switch# configure terminal
Switch(config)# evpn
Switch(config-evpn)# vni 100
Switch(config-evi)# rd auto
```

Related Commands

Vni

17.6.6 route-target

Command Purpose

Use this command to set route target for EVPN instance.
Use no format of the command to cancel the configuration.

Command Syntax

```
route-target { import | export | both } { auto | RT-VALUE }
no route-target { import | export | both } { auto | RT-VALUE }
no route-target { import | export | both | }
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>import</td>
<td>Import direction</td>
<td>-</td>
</tr>
<tr>
<td>export</td>
<td>Export direction</td>
<td>-</td>
</tr>
<tr>
<td>both</td>
<td>Import and export direction</td>
<td>-</td>
</tr>
<tr>
<td>auto</td>
<td>Automatically generates an route target</td>
<td>-</td>
</tr>
<tr>
<td>RT-VALUE</td>
<td>Route target value. ASN:nn or IP:nn</td>
<td>ASN range is 1-4294967295, nn range is 1-65535</td>
</tr>
</tbody>
</table>

Command Mode

EVI Configuration
The following example shows how to set route target:
Switch# configure terminal
Switch(config)# evpn
Switch(config-evpn)# vni 100
Switch(config-evi)# route-target both auto

**Related Commands**

Vni

17.6.7 route-target evpn

**Command Purpose**

Use this command to set route target for EVPN instance in vrf mode.
Use no format of the command to cancel the configuration.

**Command Syntax**

route-target ( import | export | both ) ( RT-VALUE ) evpn
no route-target ( import | export | both ) ( auto | RT-VALUE )
no route-target ( import | export | both )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>import</td>
<td>Import direction</td>
<td>-</td>
</tr>
<tr>
<td>export</td>
<td>Export direction</td>
<td>-</td>
</tr>
<tr>
<td>both</td>
<td>Import and export direction</td>
<td>-</td>
</tr>
<tr>
<td>RT-VALUE</td>
<td>Route target value. ASN:nn or IP:nn</td>
<td>ASN range is 1-4294967295 nn range is 1-65535</td>
</tr>
</tbody>
</table>

**Command Mode**

VRF Configuration

**Default**

None
Usage
None

Examples
The following example shows how to set route target:
Switch# configure terminal
Switch(config)#ip vrf a
Switch(config-vrf)# route-target both 1:1 evpn

Related Commands
vxlan vni

17.6.8 neighbor attribute-unchanged

Command Purpose
Use this command to advertise unchanged BGP attributes to the specified neighbor.

Use no format with this command to disable this function.

Command Syntax
neighbor (IP_ADDR | WORD) attribute-unchanged next-hop

no neighbor (IP_ADDR | WORD) attribute-unchanged next-hop

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>Specifies the address of the BGP neighbor in IPv4 format</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>WORD</td>
<td>Name of an existing peer-group</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode
Address Family Configuration

Default
None

Usage
None

Examples
The following example shows how to set nexthop unchanged attribute:
Switch# configure terminal
Switch(config)#router bgp 100
Switch(config-router)#address-family l2vpn evpn
Switch(config-router-af)# neighbor 1.1.1.1 attribute-unchanged next-hop

Related Commands
address-family l2vpn evpn
17.6.9 neighbor send-community

Command Purpose

Use this command to specify that a community attribute should be sent to a BGP neighbor.
Use no format with this command to remove the entry.

Command Syntax

neighbor (IP_ADDR | WORD) (both | extended | standard)
no neighbor (IP_ADDR | WORD) (both | extended | standard)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>Specifies the address of the BGP neighbor in IPv4 format</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>WORD</td>
<td>Name of an existing peer-group</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>both</td>
<td>Sends Standard and Extended Community attributes</td>
<td>-</td>
</tr>
<tr>
<td>extended</td>
<td>Sends Extended Community attributes</td>
<td>-</td>
</tr>
<tr>
<td>standard</td>
<td>Sends Standard Community attributes</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Address Family Configuration

Default
None

Usage
None

Examples

The following example shows how to set send-community attribute:

```
Switch# configure terminal
Switch(config)#router bgp 100
Switch(config-router)#address-family l2vpn evpn
Switch(config-router-af)#neighbor 1.1.1.1 send-community extended
```

Related Commands

address-family l2vpn evpn
17.6.10  neighbor route-reflector-client

Command Purpose

Use this command to configure the router as a BGP route reflector and configure the specified neighbor as its client.
Use the no parameter with this command to indicate that the neighbor is not a client.

Command Syntax

neighbor NEIGHBORID route-reflector-client
no neighbor NEIGHBORID route-reflector-client

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEIGHBORID</td>
<td>(A.B.C.D</td>
<td>TAG)</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>Specifies the address of the BGP neighbor in IPv4 format.</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>TAG</td>
<td>Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Address Family Configuration

Default
N/A

Usage

Route reflectors are a solution for the explosion of iBGP peering within an autonomous system. By route reflection the number of iBGP peers within an AS is reduced. Use the neighbor route-reflector-client command to configure the local router as the route reflector and specify neighbors as its client.

An AS can have more than one route reflector. One route reflector treats the other route reflector as another iBGP speaker.

Examples

$Switch# configure terminal
Switch(config)#router bgp 100
Switch(config-router)#address-family l2vpn evpn
Switch(config-router-af)# neighbor 10.10.0.72 route-reflector-client

Related Commands
N/A
17.6.11  retain route-target all

Command Purpose

Use this command to configure the bgp route would not delete when they are not duplicated into evpn instance.
Use no format of this command to cancel the configuration.

Command Syntax

retain route-target all

Command Mode

Address Family Configuration

Default

None

Usage

when the bgp would be used for transmitting the bgp route as the underlay network, it should set this configuration.

Examples

The following example shows how to set this configuration:

Switch# configure terminal
Switch(config)#router bgp 100
Switch(config-router)#address-family l2vpn evpn
Switch(config-router-af)#retain route-target all

Related Commands

Evpn

17.6.12 advertise l2vpn evpn

Command Purpose

Use this command to configure the bgp vrf instance route could be advertised into the evpn instance.
Use no format of this command to cancel the configuration.

Command Syntax

advertise l2vpn evpn
**Command Mode**

**Address Family Configuration**

**Default**

None

**Usage**

When it is needed to advertise the route of vrf instance to the evpn instance as type5 route, it should set this configuration.

**Examples**

The following example shows how to set this configuration:

Switch# configure terminal
Switch(config)#router bgp 100
Switch(config-router)#address-family ipv4 vrf a
Switch(config-router-af)#advertise l2vpn evpn

**Related Commands**

Evpn

**17.6.13 Vni**

**Command Purpose**

Use this command to create EVPN instance.

Use no format of this command to cancel the configuration.

**Command Syntax**

vni VAL

no vni VAL

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VAL</td>
<td>The ID of vni</td>
<td>1-16777215</td>
</tr>
</tbody>
</table>

**Command Mode**

EVPN Configuration

**Default**

None
Usage

The EVPN instance will be ready until both RD and route-target is set.

Examples

The following example shows how to create an EVPN instance:

```plaintext
Switch# configure terminal
Switch(config)# evpn
Switch(config-evpn)# vni 2001
Switch(config-evi)#
```

Related Commands

```
Evpn
```

**17.6.14 vxlan vni**

Command Purpose

Use this command to create EVPN instance of vrf.

Use no format of this command to cancel the configuration.

Command Syntax

```
vxlan vni VAL
no vxlan vni VAL
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VAL</td>
<td>The ID of vni</td>
<td>1-16777215</td>
</tr>
</tbody>
</table>

Command Mode

EVPN Configuration

Default

None

Usage

The EVPN instance will be ready until both RD and route-target is set.
Examples

The following example shows how to create an EVPN instance:

```plaintext
Switch# configure terminal
Switch(config)# ip vrf a
Switch(config-vrf)# vxlan vni 1000
```

Related Commands

Evpn

17.6.15 vxlan uplink

Command Purpose

Use the vxlan uplink command to enable or disable vxlan uplink port capability.

Command Syntax

`vxlan uplink (enable | disable)`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Make vxlan uplink port enable</td>
<td>-</td>
</tr>
<tr>
<td><code>disable</code></td>
<td>Make vxlan uplink port disable</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

Disable

Usage

The command is allow setting on ether type port. This command is used to decapsulated the vxlan packet for l2 vni and l3 vni

Examples

This example shows how to enable vxlan uplink on interface:

```plaintext
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# vxlan uplink enable
```

Related Commands

None
17.6.16 interface nve

Command Purpose
Use this command to create an interface nve.
Use no format of this command to cancel the configuration.

Command Syntax
interface nve IFNVE

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNVE</td>
<td>The index of nve if</td>
<td>0-3</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
There are four nves configured because of four source ip address of overlay

Examples
The following example shows how to create an interface nve:

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

Related Commands
show interface nve

17.6.17 source

Command Purpose
Use this command to set the overlay source vtep ip address of nve.
To remove the source vtep ip address of nve, use the no form of this command.

Command Syntax
source (IP_ADDR | IFNAME )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>The overlay source vtep ip address of nve, it should be a valid interface ip address.</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IFNAME</td>
<td>The overlay source interface of nve must have primary ip address</td>
<td>Aggregation, physical, vlan and loopback interface</td>
</tr>
</tbody>
</table>
Command Mode
Interface Configuration

Default
None

Usage
Overlay source vtep ip address is used to encaps and decaps overlay packets. It is recommended that the source vtep ip address is the same with some loopback interface address so that ip routing can be reachable.

Examples
The following example sets the source vtep ip address of nve:

Switch# configure terminal
Switch(config)# interface nve 1
Switch(config-if)# source 1.1.1.1

switch# show interface nve 1
Interface nve1
  Interface current state: UP
  Index 540673, Metric 0, Encapsulation VXLAN
  VRF binding: not bound
  Tunnel protocol/transport Vxlan, Status Valid
  Source 1.2.3.4 (loopback1)
  tunnel keep-vlan-tag disable
tunnel split-horizon enable
tunnel encapsulation-dscp-strategy dscp-copy
Vni 10000, protocol type bgp, Inclusive-multi(local) active
Vni 20000, protocol type bgp (associate-vrf), Inclusive-multi(local) inactive

Related Commands
None

17.6.18 member vni

Command Purpose
Use this command to bind the vni with the nve.

To unbind the vni from the nve, use the no form of this command.

Command Syntax
member vni ( VAL ) ( associate-vrf | )

no member vni ( VAL ) ( associate-vrf | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VAL</td>
<td>The vni of value</td>
<td>1-16777215</td>
</tr>
<tr>
<td>associate-vrf</td>
<td>The L3 vni of vrf</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration
**Default**

None

**Usage**

The vni without associate-vrf is L2 vni and other is L3 vni

**Examples**

The following example configure the L2 vni for nve if:

```plaintext
Switch# configure terminal
Switch(config)#interface nve 1
Switch(config-if)# member vni 10000

switch# show interface nve 1
Interface nve 1
  Interface current state: UP
  Index 540673 , Metric 0 , Encapsulation VXLAN
  VRF binding: not bound
  Tunnel protocol/transport Vxlan, Status Valid
  Source 1.2.3.4 (loopback1)
  tunnel keep-vlan-tag disable
  tunnel split-horizon enable
  tunnel encapsulation-dscp-strategy dscp-copy
  Vni 10000, protocol type bgp, Inclusive-multi(local) active
```

**Related Commands**

None

**17.6.19 dscp-strategy**

**Command Purpose**

Use the command to configure the outer ip dscp gaining mode.

**Command Syntax**

```plaintext
encapsulation-dscp-strategy ( dscp-copy | priority-map | custom-assign VALUE )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dscp-copy</td>
<td>Copy from inner ip dscp</td>
<td>-</td>
</tr>
<tr>
<td>priority-map</td>
<td>Map from priority of qos</td>
<td>-</td>
</tr>
<tr>
<td>VALUE</td>
<td>Assign dscp by users</td>
<td>0-63</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration
**Default**

Dscp-copy

**Usage**

When dscp-strategy is set priority-map, please configure QOS priority by MQC.

**Examples**

The following example sets overlay dscp-strategy as custom-assign:

```
Switch# configure terminal
Switch(config)# interface nve 1
Switch(config-if)# encapsulation-dscp-strategy custom-assign 63
```

**Related Commands**

None

**17.6.20 Virtual-mac**

**Command Purpose**

Use the virtual mac command to specify the virtual route mac address of nve vtep. Use the no form of this command to remove the virtual mac address of nve vtep.

**Command Syntax**

```
virtual-mac MAC
no virtual-mac
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC</td>
<td>The virtual mac address of remote vtep of nve</td>
<td>HHHH.HHHH.HHHH</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

None

**Usage**

The virtual mac address will be used as the inner mac address of routes for evpn firstly.
Examples

The following example sets the nve remote vtep with the virtual mac a.a.a:

```
Switch# configure terminal
Switch(config)# interface nve 1
Switch(config-if)# virtual-mac a.a.a
```

Related Commands

None

17.6.21 keep-vlan-tag

Command Purpose

Use the command to configure the nve remote vtep for keep the inner vlan tag.

Command Syntax

```
keep-vlan-tag ( enable | disable )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable keep vlan tag</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>disable keep vlan tag</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Interface Configuration

Default

Disable

Usage

None

Examples

The following example enables the remote vtep keep vlan tag of nve:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# keep-vlan-tag enable
```

Related Commands

None
17.6.22 split-horizon

Command Purpose
Use the command to configure the nve remote vtep for split-horizon.

Command Syntax
split-horizon ( enable | disable )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable split-horizon</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>disable split-horizon</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
Enable

Usage
None

Examples
The following example disables the split-horizon of overlay tunnel:
Switch# configure terminal
Switch(config)# interface nve 1
Switch(config-if)# split-horizon disable

Related Commands
None

17.6.23 evpn inclusive-multicast

Command Purpose
Use the command to configure the evpn inclusive multiple route whether it can be sent.

Command Syntax
evpn inclusive-multicast ( enable | disable )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable sending inclusive-multicast route</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>disable sending inclusive multicast route</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration
Default

Enable

Usage

None

Examples

The following example disables the sending inclusive-multicast route by nve:

Switch# configure terminal
Switch(config)# interface nve 1
Switch(config-if)# evpn inclusive-multicast disable

Related Commands

None

17.6.24  vlan arp-broadcast-suppress

Command Purpose

Use the command to enable the arp broadcast suppress of vlan. Use the no form of this command to remove the configuration.

Command Syntax

vlan <2-4094> arp-broadcast-suppress

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable arp broadcast suppress</td>
<td>-</td>
</tr>
<tr>
<td>disable</td>
<td>disable arp broadcast suppress</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

VLAN Configuration

Default

Disable

Usage

None
Examples

The following example enables arp broadcast suppress of vla 10:

```
Switch# configure terminal
Switch(config)#vlan database
Switch(config-vlan)#vlan 10 arp-broadcast-suppress enable
```

Related Commands

None

17.6.25  evpn mode

Command Purpose

Use the command to configure the evpn mode as asymmetry. Use the no form of this command to remove the configuration.

Command Syntax

```
evpn mode asymmetry
```

Command Mode

Global Configuration

Default

Symmetry

Usage

None

Examples

The following example configures the evpn mode as asymmetry:

```
Switch# configure terminal
Switch(config)#evpn mode asymmetry
```

Related Commands

None
17.6.26  vlan mac-address-tunnel learning-disable

Command Purpose
Use the command to disable the inner fdb learning of evpn tunnel. Use the no form of this command to remove the configuration.

Command Syntax
vlan <2-4094> mac-address-tunnel learning-disable

Command Mode
OVERLAY Configuration

Default
None

Usage
None

Examples
The following example configures the tunnel fdb learning disable for vlan 10:
Switch# configure terminal
Switch(config)#overlay
Switch(config-overlay)#vlan 10 mac-address-tunnel learning-disable

Related Commands
None

17.6.27  show bgp evpn

Command Purpose
Use this command to display the route information of EVPN.

Command Syntax
show bgp evpn ( all | rd VAL | vni VAL ) ( route-type ( mac-ip | inclusive-multi | ip-prefix | ) )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Display all EVPN route</td>
<td>-</td>
</tr>
<tr>
<td>rd VAL</td>
<td>Specify the rd to display EVPN route</td>
<td>Route distinguisher value. ASN:nn or IP:nn. ASN range is 1-4294967295. nn range is 1-65535</td>
</tr>
<tr>
<td>vni VAL</td>
<td>Specify the vni to display EVPN route</td>
<td>1-16777215</td>
</tr>
<tr>
<td>route-type</td>
<td>Specify the type of EVPN route</td>
<td>-</td>
</tr>
<tr>
<td>mac-ip</td>
<td>MAC/IP Advertisement Route</td>
<td>-</td>
</tr>
<tr>
<td>inclusive-multi</td>
<td>Inclusive-Multiple Advertisement Route</td>
<td>-</td>
</tr>
<tr>
<td>ip-prefix</td>
<td>ip-prefix Advertisement Route</td>
<td>-</td>
</tr>
</tbody>
</table>
**Command Mode**

Privileged EXEC

**Default**

None

**Usage**

None

**Examples**

The following example shows how to display the route information of EVPN:

Switch# show bgp evpn all

<table>
<thead>
<tr>
<th>Status codes: s suppressed, d damped, h history, * valid, &gt; best, i - internal, S Stale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Origin codes: i - IGP, e - EGP, ? - incomplete</td>
</tr>
<tr>
<td>Network</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>Route Distinguisher: 1.2001 (VNI 2001)</td>
</tr>
<tr>
<td>* &gt; [2]:[0]:[48]:[8264.c465.9400]:[32]:[12.12.12.2]/136</td>
</tr>
<tr>
<td>1.1.1.1</td>
</tr>
<tr>
<td>* &gt; [2]:[0]:[48]:[8264.c465.9400]:[32]:[12.12.12.3]/136</td>
</tr>
<tr>
<td>1.1.1.1</td>
</tr>
</tbody>
</table>

**Related Commands**

Evpn

17.6.28  show bgp evpn instance

**Command Purpose**

Use this command to display the instance information of EVPN.

**Command Syntax**

```
show bgp evpn instance ( all | vni VAL)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>all evpn instance</td>
<td>-</td>
</tr>
<tr>
<td>vni VAL</td>
<td>Secify the vni to display EVPN instance</td>
<td>1-16777215</td>
</tr>
</tbody>
</table>

**Command Mode**

Privileged EXEC
Default
None

Usage
None

Examples
The following example shows how to display the information of EVPN instance:

```
Switch# show bgp evpn instance vni 10000
Switch# show bgp evpn instance vni 10000
VVPN instance vni : 10000
  Address family : evpn
  Route Distinguisher: 1:10000(auto)
  Route Target Export: assigned
    : 1:10000
  Route Target Import: assigned
    : 1:10000
  Route Map Export : -
  Route Map Import : -
DUT2#
```

Related Commands

17.6.29 show bgp evpn neighbors

Command Purpose
Use this command to display the neighbor information of EVPN.

Command Syntax

```
show bgp evpn (neighbors IP_ADDR | summary )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>Secify the IP address of neighbor</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>summary</td>
<td>Display the summary information of EVPN neighbors</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None
Usage

None

Examples

The following example shows how to display the summary information of EVPN neighbors:

Switch# show bgp evpn summary

BGP router identifier 12.12.12.1, local AS number 1
BGP table version is 10
1 BGP AS-PATH entries
0 BGP community entries

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
1.1.1.2 4 1 946 954 10 0 0 13:35:36 0

Total number of neighbors 1

Related Commands

Evpn

17.6.30  show overlay host-information

Command Purpose

Use this command to display the host information.

Command Syntax

show overlay host-information ( vni VAL | summary )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vni VAL</td>
<td>Secify the vni to display host information, range in [1,16777215]</td>
<td>1-16777215</td>
</tr>
<tr>
<td>summary</td>
<td>Specify the summary of host information</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None
Examples

The following example shows how to display the route information of EVPN:

Switch# show overlay host-information vni 2001

<table>
<thead>
<tr>
<th>Mac</th>
<th>IP address</th>
<th>VTEP address</th>
<th>Tunnel Route</th>
</tr>
</thead>
<tbody>
<tr>
<td>8264.c465.9400</td>
<td>12.12.12.3</td>
<td>1.1.1.1</td>
<td>N</td>
</tr>
</tbody>
</table>

Related Commands

Evpn

17.6.31  show interface nve

Command Purpose

Use this command to display the interface nve information.

Command Syntax

show interface nve INDEX

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INDEX</td>
<td>The index of nve if</td>
<td>0-3</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display the nve if information:

Switch# show interface nve 1

Switch# show interface nve 1

Interface nve 1
Interface current state: UP
Index 540673, Metric 0, Encapsulation VXLAN
VRF binding: not bound
Tunnel protocol/transport Vxlan, Status Valid
Source 1.2.3.4 (loopback1)
tunnel keep-vlan-tag disable
tunnel split-horizon enable
tunnel encapsulation-dscp-strategy dscp-copy
Vni 10000, protocol type bgp, Inclusive-multi(local) active
Vni 20000, protocol type bgp (associate-vrf), Inclusive-multi(local) inactive

Related Commands

17.6.32 show overlay tunnel

Command Purpose

Use this command to display the overlay tunnel info.

Command Syntax

show overlay tunnel ( static | evpn | interface nve IFNVE )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>static</td>
<td>tunnel of static</td>
<td>-</td>
</tr>
<tr>
<td>evpn</td>
<td>tunnel of evpn</td>
<td>-</td>
</tr>
<tr>
<td>IFNVE</td>
<td>The index of nve if</td>
<td>0-3</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display the overlay tunnel information:
Switch# show overlay tunnel evpn
switch# show overlay tunnel evpn

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Vni</th>
<th>Type</th>
<th>Remote-vtep IP-Address</th>
<th>Src-Address</th>
<th>Head-end-flooding Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>10000</td>
<td>VxLAN</td>
<td>0</td>
<td>10.20.30.40</td>
<td>1.2.3.4</td>
</tr>
</tbody>
</table>
DUT2# Evpn

Related Commands
17.6.33  show overlay evpn remote-vtep

Command Purpose

Use this command to display the overlay evpn vtep info.

Command Syntax

show overlay evpn remote-vtep (interface nve IFNVE)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNVE</td>
<td>The index of nve if</td>
<td>0-3</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display the overlay tunnel information:

Switch# show overlay evpn remote-vtep interface nve 1

Related Commands

None

17.6.34  show overlay arp-suppress-information

Command Purpose

Use this command to display the entry of arp broadcast entry.
Command Syntax

show overlay arp-suppress-information

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display the arp broadcast entry:

```
Switch# show overlay arp-suppress-information
switch# show overlay arp-suppress-information
IP address        Mac        ref
-------------------------------
10.1.1.4           a239.c664.f100 1
Total: 1
```

Related Commands

None

17.6.35  show overlay mac-forwarding-information

Command Purpose

Use this command to display the remote fdb information.

Command Syntax

show overlay mac-forwarding-information ( vni VAL | summary )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vni VAL</td>
<td>Specify the vni to display host information, range in [1,16777215]</td>
<td>1-16777215</td>
</tr>
<tr>
<td>summary</td>
<td>Specify the summary of host information</td>
<td>-</td>
</tr>
</tbody>
</table>
Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display the mac forward information of EVPN:

Switch# show overlay mac-forwarding-information vni 10000

switch# show overlay mac-forwarding-information vni 10000

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac</th>
<th>IP address</th>
<th>Tunnel</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>6ae7.f8cb.7700</td>
<td>10.20.30.40</td>
<td>Y</td>
</tr>
</tbody>
</table>

Related Commands

evpn
Chapter 18 MPLS Commands

18.1 LDP Commands

18.1.1 advertise-labels for

Command Purpose
Use this command to specify which destinations have their labels advertised to LDP neighbors. Use the no parameter to specify which destinations do not have their labels advertised to LDP neighbors.

Command Syntax
advertise-labels for PREFIX_ACL to ( PEER_ACL | any )
no advertise-labels for PREFIX_ACL to ( PEER_ACL | any )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PREFIX_ACL</td>
<td>Prefix access control list name</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>PEER_ACL</td>
<td>Peer prefix list name</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>any</td>
<td>All LDP neighbors</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration

Default
The labels of all destinations are advertised to all LDP neighbors.

Usage
None

Examples
In the following example, the advertise-labels for command are used to specify which destinations have their labels advertised to all LDP neighbors:

Switch# configure terminal
Switch(config)# router ldp
Switch(config-router)# advertise-labels for prefix-acl to any

Related Commands
advertise-labels for any to none
advertise-labels for prefix-acl to peer-acl

18.1.2 clear ldp adjacency

Command Purpose
Use this command to clear an adjacency with a specified peer (IP address IP_ADDR), or to clear all adjacencies for the current LSR.

Command Syntax
clear ldp adjacency ( IP_ADDR | * )
### clear ldp adjacency

**Parameter** | **Parameter Description** | **Parameter Value**
--- | --- | ---
IP_ADDR | The address of the adjacent peer | IPv4 Address
* | Use to clear all adjacencies | -

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
In the following example, the `clear ldp adjacency` command is used to clear an adjacency with a specified peer:

```
Switch# clear ldp adjacency 123.123.123.33
```

**Related Commands**
clear ldp session
show ldp adjacency

### clear ldp session

**Command Purpose**
Use this command to clear a session established with a specified peer (IP address IP_ADDR), or to clear all sessions for the current LSR.

**Command Syntax**
clear ldp session (IP_ADDR | *)

**Parameter** | **Parameter Description** | **Parameter Value**
--- | --- | ---
IP_ADDR | The address of the adjacent peer | IPv4 Address
* | Use to clear all adjacencies | -

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
In the following example, the `clear ldp session` command is used to clear a session established with a specified peer:

```
Switch# clear ldp session 123.123.123.33
```
Related Commands
- clear ldp adjacency
- show ldp adjacency
- show ldp session

18.1.4 clear ldp statistics

Command Purpose
Use this command to clear LDP packet statistics.

Command Syntax
- clear ldp statistics

Command Mode
- Privileged EXEC

Default
None

Usage
None

Examples
In the following example, the clear ldp statistics command is used to clear LDP packet statistics:

Switch# clear ldp statistics

Related Commands
- show ldp statistics

18.1.5 clear ldp statistics advertise-labels

Command Purpose
Use this command to clear LDP advertise-labels statistics.

Command Syntax
- clear ldp statistics advertise-labels (for PREFIX_ACL) (to PEER_ACL)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PREFIX_ACL</td>
<td>Prefix access control list name</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>PEER_ACL</td>
<td>Peer prefix list name</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

Command Mode
- Privileged EXEC

Default
None
Usage
None

Examples
In the following example, the clear ldp statistics advertise-labels command is used to clear LDP advertise-labels statistics:
Switch# clear ldp statistics advertise-labels for prefix_acl to peer_acl

Related Commands
show ldp statistics advertise-labels

18.1.6 control-mode

Command Purpose
Use this command to set the control mode for label processing. Use the no parameter to revert to default control mode.

Command Syntax
control-mode ( ordered | independent )
no control-mode ( ordered | independent )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ordered</td>
<td>Sets control mode to ordered processing.</td>
<td>-</td>
</tr>
<tr>
<td>independent</td>
<td>Sets control mode to independent processing</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration

Default
Independent control

Usage
Ordered processing sets the mode to strict chain-of-command; an LSR replies to a request packet from an LSR higher in the chain only after it receives a label from an LSR lower in the chain. Independent processing sets the mode to instant replies.
In independent control mode, each LSR might advertise label mappings to its neighbors at any time. An LSR might advertise a label mapping for an FEC to its neighbors whenever it is prepared to label-switch that FEC.
In ordered control mode, an LSR may initiate the transmission of label mapping only for an FEC for which it has a label mapping for the FEC next hop, or for which the LSR is the egress.
Changes in control mode only affect labels that were sent to or received after the change was made.

Examples
In the following example, the control-mode command is used to set the control mode for label processing:
Switch# configure terminal
Switch(config)# router ldp
Switch(config-router)# control-mode ordered
18.1.7 debug ldp advertise-labels

**Command Purpose**
Use this command to debug the IP access list of LDP advertise-labels. Use the no parameter with this command to disable this function.

**Command Syntax**
dep ldp advertise-labels
no debug ldp advertise-labels

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
In the following example, the debug ldp advertise-labels command is used to debug the IP access list of LDP advertise-labels:

```
Switch# debug ldp advertise-labels
```

18.1.8 debug ldp all

**Command Purpose**
Use this command to enable all LDP troubleshooting functions. Use the no parameter with this command to disable this function.

**Command Syntax**
dep ldp all
no debug ldp all

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None
Examples
In the following example, the debug ldp all command is used to enable all LDP troubleshooting functions:

```
Switch# debug ldp all
```

Related Commands
show debugging ldp

18.1.9 debug ldp dsm

Command Purpose
Use this command to write Downstream state machine specific information to the output.

Command Syntax
debug ldp dsm
no debug ldp dsm

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
In the following example, the debug ldp dsm command is used to write Downstream state machine specific information to the output:

```
Switch# debug ldp dsm
```

Related Commands
debug ldp fsm
debug ldp packet

18.1.10 debug ldp usm

Command Purpose
Use this command to write Upstream state machine specific information to the output.

Command Syntax
debug ldp usm
no debug ldp usm

Command Mode
Privileged EXEC
Default
None

Usage
None

Examples
In the following example, the debug ldp usm command is used to write Downstream state machine specific information to the output:
Switch# debug ldp usm

Related Commands
d debug ldp fsm
d debug ldp packet

18.1.11 debug ldp events

Command Purpose
Use this command to monitor all LDP events, such as sending packets and receiving packets.

Command Syntax
d debug ldp events
d no debug ldp events

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
In the following example, the debug ldp events command is used to monitor all LDP events:
Switch# debug ldp events

2002/06/18 11:30:35 LDP: RECV packet from 192.168.3.5 port 32783
2002/06/18 11:30:35 LDP: ldp_message_hello_recv: Hello Packet received from 192.168.3.5
2002/06/18 11:30:36 LDP: ldp_message_hello_send: Sending Hello message via interface eth1. No transport address is being advertised.
2002/06/18 11:30:36 LDP: SEND to socket 13 port 646 addr 224.0.0.2
2002/06/18 11:30:36 LDP: ldp_message_hello_send: Sending Hello message via interface eth2. No transport address is being advertised.
2002/06/18 11:30:36 LDP: SEND to socket 13 port 646 addr 224.0.0.2
2002/06/18 11:30:37 LDP: Server : TCP Connection established with 192.168.3.5
2002/06/18 11:30:37 LDP: ldp_message_initialization_recv: Initialization message
Related Commands
debug ldp fsm
debug ldp packet

18.1.12 debug ldp fsm

Command Purpose
Use this command to monitor the LDP finite state machine status.

Command Syntax
ddebug ldp fsm
nno debug ldp fsm

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
In the following example, the debug ldp fsm command is used to monitor the LDP finite state machine status:

Switch# debug ldp fsm

2002/06/18 11:40:01 LDP: FSM: State changed from NON_EXISTENT to INITIALIZED for event LDP_EVENT_TCP_established
2002/06/18 11:40:01 LDP: FSM: State changed from INITIALIZED to OPENREC for event LDP_EVENT_Recv_Init_msg
2002/06/18 11:40:01 LDP: FSM: State changed from OPENREC to OPERATIONAL for event LDP_EVENT_Recv_KeepAlive_msg
2002/06/18 11:40:01 LDP: FSM: State changed from OPERATIONAL to OPERATIONAL for event LDP_EVENT_Recv_Other_msg

Related Commands
ddebug ldp packet
ddebug ldp events

18.1.13 debug ldp hexdump

Command Purpose
Use this command to write hexdump specific information to the output.
**Command Syntax**
drug ldp hexdump
no debug ldp hexdump

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
In the following example, the debug ldp hexdump command is used to write hexdump specific information to the output:

Switch# debug ldp hexdump

**Related Commands**
drug ldp fsm
drug ldp packet

---

**18.1.14 debug ldp packet**

**Command Purpose**
Use this command to monitor all sent or received packets to or from LDP peers.

**Command Syntax**
drug ldp packet
no debug ldp packet

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
In the following example, the debug ldp packet command is used to received packets to or from LDP peers:

Switch# debug ldp packet

2002/06/18 11:43:23 LDP: ldp_message_hello_send: Dump of outgoing packet
2002/06/18 11:43:23 LDP:
2002/06/18 11:43:23 LDP: PDU Version: 1
2002/06/18 11:43:23 LDP: PDU Length: 22
2002/06/18 11:43:23 LDP: LDP Identifier: 10.10.0.11:0
2002/06/18 11:43:23 LDP:
2002/06/18 11:43:23 LDP: Message U bit: 0
2002/06/18 11:43:23 LDP: Message Type: Hello Message
2002/06/18 11:43:23 LDP: Message Length: 12
2002/06/18 11:43:23 LDP: Message ID: 0x1a9
2002/06/18 11:43:23 LDP:
2002/06/18 11:43:23 LDP: TLV U bit: 0
2002/06/18 11:43:23 LDP: TLV F bit: 0
2002/06/18 11:43:23 LDP: TLV Type: Common Hello Parameters TLV
2002/06/18 11:43:23 LDP: TLV length: 4
2002/06/18 11:43:23 LDP: Hold Time: 15
2002/06/18 11:43:23 LDP: Targeted Hello: 0
2002/06/18 11:43:23 LDP: Request Send Targedetail

Related Commands
debug ldp fsm
debug ldp events

18.1.15 debug ldp qos

Command Purpose
Use this command to write Quality of Service information to the output.

Command Syntax
debug ldp qos
no debug ldp qos

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
In the following example, the debug ldp qos command is used to write Quality of Service information to the output:
Switch# debug ldp qos

Related Commands
debug ldp fsm
debug ldp packet
18.1.16 debug ldp tsm

Command Purpose
Use this command to write trunk state machine specific information to the output.

Command Syntax
debug ldp tsm
no debug ldp tsm

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
In the following example, the debug ldp tsm command is used to write trunk state machine specific information to the output:
Switch# debug ldp tsm

Related Commands
debug ldp fsm
debug ldp packet

18.1.17 debug ldp vc

Command Purpose
Use this command to debug Layer-2 Virtual Circuit information.

Command Syntax
debug ldp vc (dsm | usm | events)
no debug ldp vc (dsm | usm | events)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dsm</td>
<td>Downstream state machine</td>
<td>-</td>
</tr>
<tr>
<td>usm</td>
<td>Upstream state machine</td>
<td>-</td>
</tr>
<tr>
<td>events</td>
<td>VC events</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None
Usage
None

Examples
In the following example, the debug ldp vc events command is used to debug Layer-2 Virtual Circuit information:
Switch# debug ldp vc events

Related Commands
ddebug ldp dsm
ddebug ldp usm

18.1.18 disable-ldp

Command Purpose
Use this command to disable LDP on a specified interface.

Command Syntax
disable-ldp

Command Mode
Interface Configuration

Default
None

Usage
None

Examples
In the following example, the disable-ldp command is used to disable LDP on a specified interface:
$Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# disable-ldp

Related Commands
None

18.1.19 enable-ldp

Command Purpose
Use this command to enable LDP on a specified interface.

Command Syntax
enable-ldp
Command Mode
Interface Configuration

Default
None

Usage
None

Examples
In the following example, the enable-ldp command is used to enable LDP on a specified interface:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# enable-ldp

Related Commands
None

18.1.20 explicit-null

Command Purpose
Use this command to configure the router to send explicit-null labels for directly connected FECs instead of implicit-null labels. Implicit-nulls are the default labels.

Command Syntax
explicit-null
no explicit-null

Command Mode
Router Configuration

Default
Sends implicit-null labels

Usage
None

Examples
In the following example, the explicit-null command is used to send explicit-null labels for directly connected FECs instead of implicit-null labels:

Switch# configure terminal
Switch(config)# router ldp
Switch(config-router)# explicit-null

Related Commands
show ldp FEC
18.1.21 hello-interval

Command Purpose
Use this command to set the interval after which hello packets are sent out. Use the no parameter to revert to default hello interval.

Command Syntax
hello-interval INTERVAL
no hello-interval

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>Interval in seconds for sending periodic hello message to peers</td>
<td>1-21845</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration

Default
The default is 5 seconds.

Usage
None

Examples
In the following example, the hello-interval command is used to set the interval after which hello packets are sent out:

Switch# configure terminal
Switch(config)# router ldp
Switch(config-router)# hello-interval 35

Related Commands
hold-time
ldp hello-interval
ldp hold-time

18.1.22 hold-time

Command Purpose
Use this command to set the global value for the hold-time after which the LSR rejects adjacencies. Use the no parameter to revert to the default hold time.

Command Syntax
hold-time TIME
no hold-time

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIME</td>
<td>Specifies the hold-time value in seconds</td>
<td>3-65535</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration
Default
The default is 15 seconds.

Usage
None

Examples
In the following example, the hold-time command is used to set the global value for the hold-time after which the LSR rejects adjacencies:

Switch# configure terminal
Switch(config)# router ldp
Switch(config-router)# hold-time 635

Related Commands
- hello-interval
- ldp hello-interval
- ldp hold-time

18.1.23 keepalive-interval

Command Purpose
Use this command to set the global value for the interval after which keep-alive packets are sent out. Use the no parameter to revert to default keep-alive interval.

Command Syntax
- keepalive-interval INTERVAL
- no keepalive-interval

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>Interval in seconds for sending periodic hello message to peers</td>
<td>10-21845</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration

Default
The default is 10 seconds.

Usage
None

Examples
In the following example, the keepalive-interval command is used to set the global value for the interval after which keep-alive packets are sent out:

Switch# configure terminal
Switch(config)# router ldp
Switch(config-router)# keepalive-interval 635
Related Commands
keepalive-timeout
ldp keepalive-interval
ldp keepalive-timeout

18.1.24 keepalive-timeout

Command Purpose
Use this command to set the global value for the time-out after which sessions are rejected. Use the no parameter to revert to default keep-alive time-out.

Command Syntax
keepalive-timeout TIME
no keepalive-timeout

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIME</td>
<td>Specifies the time-out value in seconds</td>
<td>30-65535</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration

Default
The default is 30 seconds.

Usage
None

Examples
In the following example, the keepalive-timeout command is used to set the global value for the time-out after which sessions are rejected:

```
Switch# configure terminal
Switch(config)# router ldp
Switch(config-router)# keepalive-timeout 635
```

Related Commands
keepalive-timeout
ldp keepalive-interval
ldp keepalive-timeout

18.1.25 ldp hello-interval

Command Purpose
Use this command to set the interval for sending multicast Hello packets via an interface. Use the no parameter with this command to revert to the hello-interval value set for the main LDP process.
**Command Syntax**

ldp hello-interval TIME
no ldp hello-interval

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIME</td>
<td>Specifies the interval in second</td>
<td>1-21845</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

The default is 5 seconds.

**Usage**

None

**Examples**

In the following example, the ldp hello-interval command is used to set the interval for sending multicast Hello packets via an interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ldp hello-interval 635
```

**Related Commands**

hello-interval
hold-time
ldp hold-time

---

**18.1.26 ldp hold-time**

**Command Purpose**

Use this command to set the hold-time value after which the LSR rejects adjacencies. Use the no parameter to revert to the hold-time value set for the main LDP process.

**Command Syntax**

ldp hold-time TIME
no ldp hold-time

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIME</td>
<td>Specifies the interval in seconds</td>
<td>3-65535</td>
</tr>
</tbody>
</table>

**Command Mode**

Interface Configuration

**Default**

The default is 15 seconds.

**Usage**

None
Examples
In the following example, the ldp hold-time command is used to set the hold-time value after which the LSR rejects adjacencies:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ldp hold-time 635

Related Commands
hello-interval
hold-time
ldp hello-interval

18.1.27  ldp keepalive-interval

Command Purpose
Use this command to set the interval for sending keep-alive messages to the peer in order to maintain a session. Use the no parameter to revert to the keep-alive interval set for the main LDP process.

Command Syntax
ldp keepalive-interval INTERVAL
no ldp keepalive-interval

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>Specifies the interval in seconds</td>
<td>10-21845</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
The default is 10 seconds

Usage
None

Examples
In the following example, the ldp keepalive-interval command is used to set the interval for sending keep-alive messages to the peer in order to maintain a session:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ldp keepalive-interval 635

Related Commands
ldp keepalive-timeout
18.1.28  **ldp keepalive-timeout**

**Command Purpose**
Use this command to set the keep-alive time-out value for rejecting a session with a peer. Use the no parameter to revert to the keep-alive time-out set for the main LDP process.

**Command Syntax**
ldp keepalive-timeout *TIME*
no ldp keepalive-timeout

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIME</td>
<td>Specifies the value in seconds</td>
<td>30-65535</td>
</tr>
</tbody>
</table>

**Command Mode**
Interface Configuration

**Default**
The default is 30 seconds.

**Usage**
None

**Examples**
In the following example, the ldp keepalive-timeout command is used to set the keep-alive time-out value for rejecting a session with a peer:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ldp keepalive-timeout 635
```

**Related Commands**
ldp keepalive-interval

18.1.29  **ldp multicast-hellos**

**Command Purpose**
Use this command to enable multicast hello exchange on a specified interface.
Use the no parameter to disable multicast hello exchange.

**Command Syntax**
ldp multicast-hellos
no ldp multicast-hellos

**Command Mode**
Interface Configuration

**Default**
Disabled
Usage
None

Examples
In the following example, the ldp multicast-hellos command is used to enable multicast hello exchange on a specified interface:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ldp multicast-hellos

Related Commands
multicast-hellos

18.1.30 ldp targeted-peer-hello-interval

Command Purpose
Use this command to set the interval for sending unicast hello packets to targeted peers via this interface. Use the no parameter to revert to the targeted-peer hello-interval value set for the main LDP process.

Command Syntax
ldp targeted-peer-hello-interval INTERVAL
no ldp targeted-peer-hello-interval

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERVAL</td>
<td>Specifies the interval in seconds</td>
<td>1-21845</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
The default is 15 seconds.

Usage
None

Examples
In the following example, the ldp targeted-peer-hello-interval command is used to set the interval for sending unicast hello packets to targeted peers via this interface:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ldp targeted-peer-hello-interval 635

Related Commands
show ldp interface IFNAME
targeted-peer-hello-interval
18.1.31 ldp targeted-peer-hold-time

Command Purpose
Use this command to set the time-out value that is the time that the router waits before rejecting an adjacency with a targeted peer. Use the no parameter to revert to the targeted-peer value set for the main LDP process.

Command Syntax
ldp targeted-peer-hold-time TIME
no ldp targeted-peer-hold-time

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIME</td>
<td>Specifies the interval in seconds</td>
<td>3-65535</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
The default is 45 seconds.

Usage
None

Examples
In the following example, the ldp targeted-peer-hold-time command is used to set the time-out value that is the time that the router waits before rejecting an adjacency with a targeted peer:

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ldp targeted-peer-hold-time 635

Related Commands
show ldp interface IFNAME
targeted-peer-hold-time

18.1.32 router ldp

Command Purpose
This command is used to enter the LDP specific command-line mode in which global attributes for the LDP process can be set. Without this command, the LSR does not perform any LDP operations, such as sending hello packets.

Command Syntax
router ldp

Command Mode
Global Configuration

Default
None
Usage
None

Examples
In the following example, the router ldp command is used to enter the LDP specific command-line mode in which global attributes for the LDP process can be set:

Switch# configure router
Switch(config)# router ldp
Switch(config-router)#

Related Commands
None

18.1.33 router-id

Command Purpose
Use this command to set the router-id to the supplied IP address; the router uses this address to generate the LDP-ID.
Use the no parameter with this command to revert to using the first IP address configured on the box as the router-id for LDP-ID generation purposes.

Command Syntax
router-id IP_ADDR
no router-id

Command Mode
Router Configuration

Default
None

Usage
None

Examples
In the following example, the router-id command is used to set the router-id to the supplied IP address:

Switch# configure router
Switch(config)# router ldp
Switch(config-router)# router-id 123.123.123.8

Related Commands
None
18.1.34 show debugging ldp

**Command Purpose**
Use this command to display the status of the debugging of the LDP system.

**Command Syntax**
show debugging ldp

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
In the following example, the show debugging ldp command is used to display the status of the debugging of the LDP system:

```
Switch# show debugging ldp
LDP debugging status:
LDP event debugging is on
LDP packet debugging is on
LDP finite state machine debugging is on
LDP pdu hexdump debugging is on
LDP downstream state machine debugging is on
LDP upstream state machine debugging is on
LDP trunk state machine debugging is on
LDP QoS debugging is on
LDP CSPF debugging is on
LDP VC USM debugging is on
LDP VC DSM debugging is on
LDP NSM debugging is on
LDP Advertise-labels debugging is on
```

**Related Commands**
None

18.1.35 show ldp

**Command Purpose**
Use this command to display basic LDP attributes defined for the current LSR.

**Command Syntax**
show ldp
**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
The following is a sample output from the show ldp command displaying basic LDP attributes:

```
Switch# show ldp

Router ID : 10.10.0.11
LDP Version : 1
Global Merge Capability : N/A
Label Advertisement Mode : Downstream Unsolicited
Label Retention Mode : Liberal
Label Control Mode : Independent
Loop Detection : Off
Loop Detection Count : 0
Request Retry : Off
Propagate Release : Disabled
Hello Interval : 5
Targeted Hello Interval : 15
Hold time : 15
Targeted Hold time : 45
Keepalive Interval : 10
Keepalive Timeout : 30
Request retry Timeout : 5
Targeted Hello Receipt : Disabled
Transport Address : N/A
Transport Interface : N/A
Import BGP routes : No
```

**Related Commands**
None

**18.1.36  show ldp adjacency**

**Command Purpose**
Use this command to display all the adjacencies for the current LSR.

**Command Syntax**
```
show ldp adjacency
```
Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
In the following example, the show ldp adjacency command is used to display all the adjacencies for the current LSR:

```
Switch# show ldp adjacency
IP Address Interface Name Holdtime LDP ID
192.168.3.5 eth1 15 10.10.0.18:0
192.168.4.5 eth2 15 10.10.0.18:0
```

Related Commands
None

18.1.37 show ldp advertise-labels

Command Purpose
Use this command to display the IP access list of LDP advertise-labels.

Command Syntax
show ldp advertise-labels

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
In the following example, the show ldp advertise-labels command is used to display the IP access list of LDP advertise-labels:

```
Switch# show ldp advertise-labels
Advertisement spec:
Prefix acl = pfx1; Peer acl = pfx1
Prevent the distribution of any assigned labels
```
18.1.38  show ldp downstream

Command Purpose
Use this command to display the status of all downstream sessions and the label information exchanged.

Command Syntax
show ldp downstream

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
In the following example, the show ldp downstream command is used to display the status of all downstream sessions and the label information exchanged:

Switch# show ldp downstream
Session peer 192.168.11.50:
Downstream state: Established Label: impl-null RequestID: 0 Peer:
192.168.11.50 Attr:
Downstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.11.50 Attr:
Downstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.11.50 Attr:
Downstream state: Established Label: 20 RequestID: 0 Peer: 192.168.11.50 Attr:
Session peer 192.168.13.60:
Downstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.13.60 Attr:
Downstream state: Established Label: 16 RequestID: 0 Peer: 192.168.13.60 Attr:
Downstream state: Established Label: 17 RequestID: 0 Peer: 192.168.13.60 Attr:
Downstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.13.60 Attr:
Downstream state: Established Label: 18 RequestID: 0 Peer: 192.168.13.60 Attr:
Downstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.13.60 Attr:
Downstream state: Established Label: 20 RequestID: 0 Peer: 192.168.13.60 Attr:

Related Commands
None
18.1.39  show ldp fec

Command Purpose
Use the following command to display all FECs known to the current LSR.

Command Syntax
show ldp fec ( host | prefix )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>The host FEC</td>
<td>-</td>
</tr>
<tr>
<td>prefix</td>
<td>The prefix FEC</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
In the following example, the show ldp fec command is used to display all FECs known to the current LSR:

```
Switch# show ldp fec

LSR codes : E/N - LSR is egress/non-egress for this FEC,
L - LSR received a label for this FEC,
> - LSR will use this route for the FEC
Code FEC Session Out Label Nexthop Addr
E > 10.10.0.0/24 non-existent none connected
NL 10.10.0.0/24 192.168.3.5 impl-null connected
E > 192.168.3.0/24 non-existent none connected
NL 192.168.3.0/24 192.168.3.5 impl-null connected
E > 192.168.4.0/24 non-existent none connected
NL 192.168.4.0/24 192.168.3.5 impl-null connected
NL 192.168.5.0/24 192.168.3.5 impl-null invalid
```

Related Commands
None

18.1.40  show ldp interface

Command Purpose
Use this command to display information for all interfaces, or detailed information for a specific interface.

Command Syntax
show ldp interface ( IFNAME )
Parameter | Parameter Description | Parameter Value
--- | --- | ---
IFNAME | The name of the interface, the format follows below: eth-0-1, agg1, vlan1, etc | Support physical/aggregation/loopback/vlan/tunnel ports

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
In the following example, the show ldp interface command is used to display detailed information for a specific interface:

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

Status : Enabled
Primary IP Address : 192.168.3.4
Interface Type : Ethernet
Label Merge Capability : Merge Capable
Hello Interval : 5
Targeted Hello Interval : 15
Hold Time : 15
Targeted Hold Time : 45
Keepalive Interval : 10
Keepalive Timeout : 30
Advertisement Mode : Downstream On Demand
Label Retention Mode : Liberal
Administrative Groups : Cen1: Cen2

**Related Commands**
None

**18.1.41 show ldp lsp**

**Command Purpose**
Use this command to display LDP LSP and, optionally, advertise-label information.

**Command Syntax**
show ldp lsp

**Command Mode**
Privileged EXEC
**Default**
None

**Usage**
None

**Examples**
In the following example, the show ldp lsp command is used to display LDP LSP and, optionally, advertise-label information:

```
Switch# show ldp lsp

Advertisement spec:
Prefix acl = pfx1; Peer acl = pfx1
Prevent the distribution of any assigned labels
FEC IPV4:1.1.1.0/30 -> 0.0.0.0
Downstream state: Established Label: impl-null RequestID: 0 Peer: 50.50.50.50 Attr:
Advert acl(s): Prevent the distribution of any assigned labels
FEC IPV4:3.3.3.0/30 -> 0.0.0.0
Advert acl(s): Prevent the distribution of any assigned labels
FEC IPV4:10.30.0.0/24 -> 0.0.0.0
Downstream state: Established Label: impl-null RequestID: 0 Peer: 50.50.50.50 Attr:
Advert acl(s): Prevent the distribution of any assigned labels
FEC IPV4:50.50.50.32 -> 1.1.1.1
Advert acl(s): Prefix acl = pfx1; Peer acl = pfx1
FEC IPV4:55.55.55.32 -> 3.3.3.2
Advert acl(s): Prevent the distribution of any assigned labels
FEC IPV4:169.254.0.0/16 -> 0.0.0.0
Downstream state: Established Label: impl-null RequestID: 0 Peer: 50.50.50.50 Attr:
Advert acl(s): Prevent the distribution of any assigned labels
```

**Related Commands**
```
show ldp lsp host
show ldp lsp prefix
show ldp lsp cr-lsp
```

**18.1.42 show ldp mpls-vpws**

**Command Purpose**

**Command Syntax**
```
show ldp mpls-l2-circuit ( detail | Virtual_Circuit_ID )
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Show detailed information</td>
<td>-</td>
</tr>
<tr>
<td>Virtual_Circuit_ID</td>
<td>Specifies the VPWS identifier</td>
<td>1-4294967295</td>
</tr>
</tbody>
</table>
**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
Switch# show ldp mpls-vpws detail
Switch# show ldp mpls-vpws 34 detail

**Related Commands**
None

**18.1.43 show ldp session**

**Command Purpose**
Use this command to display sessions established between the current LSR and other LSRs.

**Command Syntax**
show ldp session [ IP_ADDR ]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>The IPv4 address of the peer for which information is to be shown</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
In the following example, the show ldp session command is used to display sessions established between the current LSR and other LSRs:
Switch# show ldp session

Peer IP Address IF Name My Role State KeepAlive
192.168.11.50 eth1 Passive OPERATIONAL 30
192.168.13.60 eth2 Passive OPERATIONAL 30

In the following example, the show ldp session command is used to display sessions established between the current LSR and other LSRs:
Switch# show ldp session 192.168.3.5
Session state : OPERATIONAL
Session role: Passive
TCP Connection: Established
IP Address for TCP: 192.168.3.5
Interface being used: eth1
Peer LDP ID: 10.10.0.18:0
Adjacencies: 192.168.3.5 192.168.4.5
Advertisement mode: Downstream Unsolicited
Label retention mode: Liberal
Keepalive Timeout: 30
Reconnect Interval: 15
Address List received: 192.168.3.5 192.168.4.5
Received Labels: Fec Label Maps To
IPV4:10.10.0.0/24 impl-null none
IPV4:192.168.3.0/24 impl-null none
IPV4:192.168.4.0/24 impl-null none
IPV4:192.168.5.0/24 impl-null none
Sent Labels: Fec Label Maps To
IPV4:10.10.0.0/24 impl-null none
IPV4:192.168.3.0/24 impl-null none
IPV4:192.168.4.0/24 impl-null none
IPV4:192.168.5.0/24 impl-null none

Switch# show ldp session 192.168.3.5

Session state: OPERATIONAL
Session role: Passive
TCP Connection: Established
IP Address for TCP: 192.168.3.5
Interface being used: eth1
Peer LDP ID: 10.10.0.18:0
Adjacencies: 192.168.3.5 192.168.4.5
Advertisement mode: Downstream Unsolicited
Label retention mode: Liberal
Keepalive Timeout: 30
Reconnect Interval: 15
Address List received: 192.168.3.5 192.168.4.5
Received Labels: Fec Label Maps To
IPV4:10.10.0.0/24 impl-null none
IPV4:192.168.3.0/24 impl-null none
IPV4:192.168.4.0/24 impl-null none
IPV4:192.168.5.0/24 impl-null none
Sent Labels: Fec Label Maps To
IPV4:10.10.0.0/24 impl-null none
IPV4:192.168.3.0/24 impl-null none
IPV4:192.168.4.0/24 impl-null none

Related Commands
None

18.1.44 show ldp statistics

Command Purpose
Use this command to display LDP packet statistics.

Command Syntax
show ldp statistics (advertise-labels | )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>advertise-labels</td>
<td>Count per each operation filtered by an advertisement list.</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
In the following example, the show ldp statistics command is used to display LDP packet statistics:

Switch# show ldp statistics

PacketType Total
Sent Received
Notification 0 0
Hello 3980 0
Initialization 1 1
Keepalive 1932 1932
Address 1 1
Address Withdraw 0 0
Label Mapping 7 7
Label Request 0 0
Label Withdraw 1 0
Label Release 0 1
Request About 0 0

In the following example, the show ldp statistics command is used to display LDP packet statistics:
Switch# show ldp statistics advertise-labels
Advertisement spec:
Prefix acl = pf1; Peer acl = pf1
Deny : Label Mapping = 2
Label Request = 0
Prevent the distribution of any assigned labels
Deny : Label Mapping = 9
Label Request = 3

Switch# show ldp statistics advertise-labels
Advertisement spec:
Prefix acl = pf1; Peer acl = pf1
Deny : Label Mapping = 2
Label Request = 0
Prevent the distribution of any assigned labels
Deny : Label Mapping = 9
Label Request = 3

**Related Commands**
clear ldp statistics advertise-labels

**18.1.45 show ldp targeted-peers**

**Command Purpose**
Use this command to display the list of targeted peers configured on the current LSR.

**Command Syntax**
show ldp targeted-peers

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
In the following example, the show ldp targeted-peers command is used to display the list of targeted peers configured on the current LSR:

```
Switch# show ldp targeted-peers

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.3</td>
<td>eth-0-9</td>
</tr>
</tbody>
</table>
```
Related Commands
None

18.1.46  show ldp upstream

Command Purpose
Use this command to display the status of all upstream sessions and label information exchanged.

Command Syntax
show ldp upstream

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
In the following example, the show ldp upstream command is used to display the status of all upstream sessions and label information exchanged:

Switch# show ldp targeted-peers

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.3</td>
<td>eth-0-9</td>
</tr>
</tbody>
</table>

Related Commands
None

18.1.47  show memory ldp

Command Purpose
Use this command to display memory statistics for the LDP.

Command Syntax
show memory ldp

Command Mode
Privileged EXEC

Default
None
Usage
None

Examples
In the following example, the show memory ldp command is used to display memory statistics for the LDP:

Switch# show ldp upstream

Session peer 192.168.11.50:
Upstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.11.50 Attr:
Upstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.11.50 Attr:
Upstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.11.50 Attr:
Session peer 192.168.13.60:
Upstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.13.60 Attr:
None
Upstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.13.60 Attr:
None
Upstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.13.60 Attr:
None
Upstream state: Established Label: 16 RequestID: 0 Peer: 192.168.13.60 Attr: None
Upstream state: Established Label: 17 RequestID: 0 Peer: 192.168.13.60 Attr: None
Upstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.13.60 Attr:
None
Upstream state: Established Label: 18 RequestID: 0 Peer: 192.168.13.60 Attr: None

Related Commands
None

18.1.48 targeted-peer

Command Purpose
Use this command to specify or delete a targeted LDP peer.

Command Syntax
targeted-peer IP_ADDR
no targeted-peer IP_ADDR

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>Specifies the IPv4 address of the targeted peer</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration

Default
None
Usage
None

Examples
In the following example, the targeted-peer command is used to specify a targeted LDP peer:

```
Switch# configure terminal
Switch(config)# router ldp
Switch(config-router)# targeted-peer 10.10.10.10
```

Related Commands
None

18.1.49 targeted-peer-hello-interval

Command Purpose
Use this command to set the interval for sending unicast hello packets to targeted peers. Use the no parameter with this command to revert to the default targeted-peer hello-interval value.

Command Syntax
```
targeted-peer-hello-interval INTERVAL
no targeted-peer-hello-interval
```

Parameter Description | Parameter Value
---|---
INTERVAL | Specifies the interval in seconds | 1-21845

Command Mode
Router Configuration

Default
The default is 15 seconds.

Usage
None

Examples
In the following example, the targeted-peer-hello-interval command is used to set the interval for sending unicast hello packets to targeted peers:

```
Switch# configure terminal
Switch(config)# router ldp
Switch(config-router)# targeted-peer-hello-interval 100
```

Related Commands
show ldp
targeted-peer-hello-interval
18.1.50 targeted-peer-hello-receipt

Command Purpose
Use this command to toggle the receipt of targeted hello packets. Use the no parameter to disable the processing of targeted hello packets.

Command Syntax
targeted-peer-hello-receipt
no targeted-peer-hello-receipt

Command Mode
Router Configuration

Default
None

Usage
None

Examples
In the following example, the targeted-peer-hello-receipt command is used to toggle the receipt of targeted hello packets:

```
Switch# configure router
Switch(config)# router ldp
Switch(config-router)# targeted-peer-hello-receipt
```

Related Commands
None

18.1.51 targeted-peer-hold-time

Command Purpose
Use this command to set the time-out value that is the time that the router waits before rejecting an adjacency with targeted peers. Use the no parameter to revert to the default targeted-peer hold-time value.

Command Syntax
targeted-peer-hold-time TIME
no targeted-peer-hold-time

```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIME</td>
<td>Specifies the interval in seconds</td>
<td>3-65535</td>
</tr>
</tbody>
</table>
```

Command Mode
Router Configuration

Default
The default is 45 seconds.
Usage
None

Examples
In the following example, the targeted-peer-hold-time command is used to set the time-out value that is the time that the router waits before rejecting an adjacency with targeted peers:

```bash
Switch# configure terminal
Switch(config)# router ldp
Switch(config-router)# targeted-peer-hold-time 100
```

Related Commands
show ldp
ldp targeted-peer-hold-time

18.1.52 transport-address

Command Purpose
Use this command to configure the transport address for a label space. Use the no parameter to stop using the transport-address as the IPv4 transport address. If the label-space is not specified in either form of this command, a label-space of zero is assumed.

Command Syntax
transport-address IP_ADDR
no transport-address

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>The IPv4 address to be used as the transport address. Only addresses bound to a loopback interface are valid for manual transport address configuration.</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

Command Mode
Router Configuration

Default
By default, transport addresses are chosen for label spaces. These addresses might either be bound to a loopback interface, or to a physical interface that is bound to the label space in question.

Usage
None

Examples
In the following example, the transport-address command is used to configure the transport address for a label space:

```bash
Switch# configure router
Switch(config)# router ldp
Switch(config-router)# transport-address 10.10.0.5
```
Related Commands
None

18.1.53  show ldp vpls

Command Purpose
Use this command to display information about all VPLS instances. Specify the VPLS ID to display information about a specific VPLS instance.

Command Syntax
show ldp vpls (detail | VPLS_ID)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Show detailed information</td>
<td>-</td>
</tr>
<tr>
<td>VPLS_ID</td>
<td>Specifies the VPLS identifier</td>
<td>1-4294967295</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
In the following example, the show ldp vpls command is used to display information about all VPLS instances:

Switch# show ldp vpls

VPLS-ID Peer Address State Type Label-Sent Label-Rcvd
1 192.168.0.80 Up vpls 16 640
1 192.168.0.90 Up vpls 18 642
2 192.168.0.80 Up vpls 19 641
2 192.168.0.90 Up vpls 17 643

Related Commands
None

18.2  MPLS Commands

18.2.1  mpls enable-all-interfaces

Command Purpose
Use this command to enable or disable all the L3 interfaces' label switch function.
Command Syntax
mpls enable-all-interfaces
mpls disable-all-interfaces

Command Mode
Global Configuration

Default
Label switch function is disabled.

Usage
None

Examples
In the following example, the mpls disable-all-interfaces command is used to disable all the L3 interfaces’ label switch function:
Switch# configure terminal
Switch(config)# mpls disable-all-interfaces

Related Commands
None

18.2.2 label-switching

Command Purpose
Use this command to enable or disable an interface’s label switch function.

Command Syntax
label-switching
no label-switching

Command Mode
Interface Configuration

Default
Label switch function is disabled.

Usage
None

Examples
In the following example, the label-switching command is used to enable an interface’s label switch function:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# label-switching
Related Commands
None

18.2.3 show mpls interface

Command Purpose
Use this command to display interfaces bound to MPLS interface.

Command Syntax
show mpls interface (IFNAME )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>The name of the interface, the format follows below: eth-0-1, agg1, vlan1, etc</td>
<td>Support physical/aggregation/vlan ports</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
In the following example, the show mpls interface command is used to display interfaces bound to MPLS interface:

Switch# show mpls interface eth-0-9

Interface eth-0-9
   Label switching is enabled with label-space 0
   minimum label value configured is 16
   maximum label value configured is 4095
   In-labels used:0, Out-labels used:0

Related Commands
None

18.2.4 mpls lsp-model

Command Purpose
Use this command to configure the model of mpls lsp

Command Syntax
mpls lsp-model ( uniform | pipe ( exp EXP ) | short-pipe ( exp EXP ) ) ( domain DOMAINDID )
no mpls lsp-model
### Command Mode

**Global Configuration**

### Default

Uniform mode

### Usage

None

### Examples

Configuration the mode of MPLS LSP Model:

```bash
Switch# configure terminal
Switch(config)# mpls lsp-model short-pipe exp 7 domain 1
```

### Related Commands

#### 18.2.5 mpls ilm-entry

**Command Purpose**

Use this command to add or delete the static ILM entry.

**Command Syntax**

- `mpls ilm-entry swap INLABEL IP_ADDR OUTLABEL`
- `mpls ilm-entry php INLABEL IP_ADDR`
- `mpls ilm-entry pop INLABEL`
- `no mpls ilm-entry INLABEL`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INLABEL</td>
<td>Incoming label</td>
<td>16-1048575</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>Next hop ip address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>OUTLABEL</td>
<td>Outgoing label</td>
<td>0(explicit null),3(implicit null),16-1048575</td>
</tr>
</tbody>
</table>

**Command Mode**

**Global Configuration**

**Default**

None
Usage
None

Examples
In the following example, the mpls ilm-entry command is used to configure one static ILM entry:

```
Switch# configure terminal
Switch(config)# mpls ilm-entry swap 100 12.12.12.2 200
Switch(config)# mpls ilm-entry php 101 12.12.12.20
Switch(config)# mpls ilm-entry pop 102
```

Related Commands
None

18.2.6 mpls mtu

Command Purpose
Use this command to set mpls mtu.

Command Syntax
```
mpls mtu MTU-VALUE
no mpls mtu
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTU-VALUE</td>
<td>MTU value</td>
<td>68-9216</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
None

Usage
None

Examples
In the following example, the mpls mtu command is used to configure mpls mtu:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# mpls mtu 1600
```

Related Commands
Mtu

18.2.7 show mpls ilm-database

Command Purpose
Use this command to display MPLS Incoming Label Map table for detail.
Command Syntax
show mpls ilm-database

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
In the following example, the show mpls ilm-database command is used to display MPLS Incoming Label Map table for detail:

```
Switch# show mpls ilm-database
Codes: > - selected ILM, p - stale ILM, B - BGP ILM, K - CLI ILM,
L - LDP ILM, R - RSVP-TE ILM, S - SNMP ILM, I - IGP-Shortcut,
U - unknown ILM

<table>
<thead>
<tr>
<th>Code</th>
<th>FEC</th>
<th>I/O Label</th>
<th>Nexthop</th>
<th>Out-Intf</th>
</tr>
</thead>
<tbody>
<tr>
<td>L&gt;</td>
<td>5.5.5.0/24</td>
<td>1024/3</td>
<td>3.3.3.2</td>
<td>eth-0-17</td>
</tr>
</tbody>
</table>
```

Related Commands
show mpls ilm-forwarding

18.2.8 show mpls ilm-forwarding

Command Purpose
Use this command to display MPLS Incoming Label Map table.

Command Syntax
show mpls ilm-forwarding

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
In the following example, the show mpls ilm-forwarding command is used to display MPLS Incoming Label Map table:

```
Switch# show mpls ilm-forwarding
```
### Related Commands

- show mpls ilm-database

### 18.2.9 mpls ftn-entry

#### Command Purpose

Use this command to add or delete the static FTN entry.

#### Command Syntax

```
mpls ftn-entry (IP_ADDR IP_ADDR_MASK | IP_ADDR/IP_MASK_LEN) OUTLABEL NEXTHOP
no mpls ftn-entry (IP_ADDR IP_ADDR_MASK | IP_ADDR/IP_MASK_LEN) NEXTHOP
```

#### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>IP Address of FEC</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IP_ADDR_MASK</td>
<td>IP Address mask of FEC</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IP_MASK_LEN</td>
<td>IP Address mask length of FEC</td>
<td>1-32</td>
</tr>
<tr>
<td>OUTLABEL</td>
<td>Outgoing label</td>
<td>0(explicit null),3(implicit null),16-1048575</td>
</tr>
<tr>
<td>NEXTHOP</td>
<td>Nexthop ip address</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

#### Command Mode

Global Configuration

#### Default

None

#### Usage

None

#### Examples

In the following example, the mpls ftn-entry command is used to configure one static FTN entry:

```
Switch# configure terminal
Switch(config)# mpls ftn-entry 200.200.200.0/24 200 12.12.12.2
```

#### Related Commands

None

### 18.2.10 show mpls ftn-database

#### Command Purpose

Use this command to display MPLS Forwarding table for detail.

#### Command Syntax

```
show mpls ftn-database
```

---

<table>
<thead>
<tr>
<th>FEC</th>
<th>I/O Label</th>
<th>Nexthop</th>
<th>Out-Intf</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.5.0/24</td>
<td>1024/3</td>
<td>3.3.3.2</td>
<td>eth-0-17</td>
</tr>
</tbody>
</table>

---
**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
In the following example, the show mpls ftn-database command is used to display MPLS Forwarding table for detail:

```
Switch# show mpls ftn-database
```

<table>
<thead>
<tr>
<th>Code</th>
<th>FEC</th>
<th>Out-Label</th>
<th>Nexthop</th>
<th>Out-Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>K</td>
<td>19.1.1.0/24</td>
<td>0</td>
<td>172.10.1.2</td>
<td></td>
</tr>
</tbody>
</table>

**Related Commands**
None

**18.2.11 show mpls ftn-forwarding**

**Command Purpose**
Use this command to display MPLS Forwarding table.

**Command Syntax**
```
show mpls ftn-forwarding
```

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
In the following example, the show mpls ftn-forwarding command is used to display MPLS Forwarding table:

```
Switch# show mpls ftn-forwarding
```

<table>
<thead>
<tr>
<th>FEC</th>
<th>Out-Label</th>
<th>Nexthop</th>
<th>Out-Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.3.0/24</td>
<td>3</td>
<td>2.2.2.2</td>
<td>eth-0-9</td>
</tr>
<tr>
<td>5.5.5.0/24</td>
<td>1024</td>
<td>2.2.2.2</td>
<td>eth-0-9</td>
</tr>
</tbody>
</table>
Related Commands
show mpls ftn-database

18.2.12 mpls lsp-tunneling

Command Purpose
Use this command to add or delete the ILM tunnel entry.

Command Syntax
mpls lsp-tunneling INLABEL OUTLABEL IP_ADDR/IP_MASK_LEN
no mpls lsp-tunneling INLABEL

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INLABEL</td>
<td>Incoming label</td>
<td>16-1048575</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>Tunnel FEC IP address</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IP_MASK_LEN</td>
<td>Tunnel FEC IP address mask</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>OUTLABEL</td>
<td>Outgoing label</td>
<td>0(explicit null),3(implicit null),16-1048575</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
None

Examples
In the following example, the mpls lsp-tunneling command is used to specify one ILM to tunnel:

Switch# configure terminal
Switch(config)# mpls lsp-tunneling 100 300 200.200.200.0/24

Related Commands
None

18.2.13 show mpls lsp-tunneling

Command Purpose
Use this command to display MPLS LSP-Tunneling.

Command Syntax
show mpls lsp-tunneling

Command Mode
Privileged EXEC
Default
None

Usage
None

Examples
In the following example, the show mpls lsp-tunneling command is used to display MPLS LSP-Tunneling:

```
Switch1# show mpls lsp-tunneling
```

Codes: > - selected ILM

<table>
<thead>
<tr>
<th>Code</th>
<th>I/O Label</th>
<th>FEC</th>
<th>Out-Intf</th>
</tr>
</thead>
<tbody>
<tr>
<td>200/300</td>
<td>5.5.5.0/24</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

Related Commands
None

18.2.14 mpls map-route

Command Purpose
Use this command to specify one FEC mapped to a FTN entry.

Command Syntax
```
mpls map-route (IP_ADDR/IP_MASK_LEN | IP_ADDR/IP_ADDR_MASK) (FEC_IP_ADDR/FEC_IP_MASK_LEN | FEC_IP_ADDR FEC_IP_MASK)
```
```
no mpls map-route (IP_ADDR/IP_MASK_LEN | IP_ADDR/IP_ADDR_MASK)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>IPv4 prefix to be mapped</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IP_ADDR_MASK</td>
<td>IPv4 mask of prefix to be mapped</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IP_MASK_LEN</td>
<td>IPv4 mask length of prefix to be mapped</td>
<td>1-32</td>
</tr>
<tr>
<td>FEC_IP_ADDR</td>
<td>IPv4 Forwarding Equivalence Class for route to be mapped to</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>FEC_IP_MASK</td>
<td>IPv4 Forwarding Equivalence Class mask for route to be mapped to</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>FEC_IP_MASK_LEN</td>
<td>IPv4 Forwarding Equivalence Class mask length for route to be mapped to</td>
<td>1-32</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
None
Examples

In the following example, the mpls map-route command is used to specify one FEC mapped to a FTN entry and mapped to a tunnel:

Switch# configure terminal
Switch(config)# mpls map-route 100.100.0/24 200.200.0/24
Switch(config)# mpls map-route 101.101.0/24 tunnel tun1

Related Commands

mpls ftn-entry (IP_ADDR | IP_ADDR/MASK | IP_ADDR/IP_MASK_LEN) OUTLABEL IP_ADDR

18.2.15 show mpls map-routes

Command Purpose

Use this command to display mapped MPLS routes.

Command Syntax

show mpls mapped-routes

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

In the following example, the show mpls mapped-routes command is used to display mapped MPLS routes:

```
Switch# show mpls map-routes
Mapped-route IPv4 FEC
12.12.12.0/24 -
```

Related Commands

None

18.3 VPLS Commands

18.3.1 mpls vpls

Command Purpose

Use this command to create a VPLS instance and come into the VPLS instance mode. This command will create a VPLS instance, and come into this instance mode. If the instance have been created, without inputting the VPLS-ID, it comes into the instance mode without creating VPLS instance.

Command Syntax

mpls vpls NAME VPLS-ID (whitelist) (ac-vlan-operation)
no mpls vpls NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Identifying string for VPLS instance</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>VPLS-ID</td>
<td>Identifying value for VPLS instance</td>
<td>1-4294967295</td>
</tr>
<tr>
<td>whitelist</td>
<td>Enable whitelist function</td>
<td>-</td>
</tr>
<tr>
<td>ac-vlan-operation</td>
<td>Keep vlan unchange function</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**
Global Configuration

**Default**
None

**Usage**
None

**Examples**
In the following example, the mpls vpls command is used to create a VPLS instance and come into the VPLS instance mode:

Switch# configure terminal
Switch(config)# mpls vpls vpls1 1
Switch(config-vpls)#

**Related Commands**
None

18.3.2 vpls-description

**Command Purpose**
Use this command to add characters describing for VPLS instance.

**Command Syntax**

```text
vpls-description LINE
no vpls-description
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LINE</td>
<td>Characters describing the VPLS instance</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

**Command Mode**
VPLS Configuration

**Default**
None

**Usage**
None
Examples
In the following example, the vpls-description command is used to add characters describing for VPLS instance:

Switch# configure terminal
Switch(config)# mpls vpls vpls1 1
Switch(config-vpls)# vpls-description this is a good vpls instance

Related Commands
None

18.3.3 vpls-mtu

Command Purpose
Use this command to set mtu for VPLS instance. If set the MTU value for the VPLS instance, LDP will advertise this value to peers in the instance.

Command Syntax
vpls-mtu MTU
no vpls-mtu

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTU</td>
<td>MTU value for the VPLS instance</td>
<td>576-65535</td>
</tr>
</tbody>
</table>

Command Mode
VPLS Configuration

Default
None

Usage
None

Examples
In the following example, the vpls-mtu command is used to set mtu for VPLS instance:

Switch# configure terminal
Switch(config)# mpls vpls vpls1 1
Switch(config-vpls)# vpls-mtu 55555

Related Commands
None

18.3.4 vpls-peer

Command Purpose
Use this command to add a remote PE for VPLS instance. If configure this command use key word manual, the PW to this peer will not issue by LDP or BGP, otherwise, the PW issued by LDP or BGP, can not create PW fib manually.
Command Syntax
vpls-peer IP_ADDR ( raw | tagged ) ( control-word | ) ( manual | ) ( upd | )
no vpls-peer IP_ADDR

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_ADDR</td>
<td>IP address of the peer node to be added</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>raw</td>
<td>Set Peer Virtual Circuits type to Raw mode</td>
<td>-</td>
</tr>
<tr>
<td>tagged</td>
<td>Set Peer Virtual Circuits type to Tagged mode</td>
<td>-</td>
</tr>
<tr>
<td>control-word</td>
<td>Control-word for Peer Virtual Circuits</td>
<td>-</td>
</tr>
<tr>
<td>manual</td>
<td>PW for peer will created manually</td>
<td>-</td>
</tr>
<tr>
<td>upe</td>
<td>User facing Provider Edge</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
VPLS Configuration

Default
None

Usage
None

Examples
In the following example, the vpls-peer command is used to add a remote PE for VPLS instance:
Switch# configure terminal
Switch(config)# mpls vpls vpls1 1
Switch(config-vpls)# vpls-peer 100.100.100.1 raw manual

Related Commands
no vpls-peer

18.3.5 vpls-fib-add

Command Purpose
Use this command to add a static PW for a PE in a VPLS instance. The peer should be added in VPLS instance use key-word “manual”.

Command Syntax
vpls-fib-add NAME peer IP_ADDR IN-LABLE OUT-LABEL
vpls-fib-delete NAME peer IP_ADDR

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Identifying string for VPLS instance</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>IP address of PE</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>IN-LABLE</td>
<td>Incoming label</td>
<td>16-1048575</td>
</tr>
<tr>
<td>OUT-LABEL</td>
<td>Outgoing label</td>
<td>16-1048575</td>
</tr>
</tbody>
</table>
Command Mode
Global Configuration

Default
None

Usage
None

Examples
In the following example, the vpls-fib-add command is used to add a static PW for a PE in a VPLS instance:

Switch# configure terminal
Switch(config)# vpls-fib-add vpls1 peer 100.100.100.1 101 102

Related Commands
vpls-fib-delete

18.3.6 mpls-vpls

Command Purpose
Use this command to bind an interface to a VPLS instance. The interface can not bind to same VPLS instance twice with different vlan tag; the interface can not bind to VPLS instance and MPLS Layer 2 Virtual Circuit both.

Command Syntax
mpls-vpls NAME ( vlan VLANID ( cvlan CVLANID ( bundling | ) | ethernet ) ( etree-leaf | ) ( vlan-operation-table VLAN_OP_TBL_NAME | ) )
no mpls-vpls NAME ( vlan VLANID )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Identifying string for VPLS instance</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>VLANID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>CVLANID</td>
<td>Customer ethernet VLAN</td>
<td>1-4094</td>
</tr>
<tr>
<td>bundling</td>
<td>Enable bundle function</td>
<td>-</td>
</tr>
<tr>
<td>ethernet</td>
<td>Ethernet Mode</td>
<td>-</td>
</tr>
<tr>
<td>etree-leaf</td>
<td>Leaf-ACs in an ETREE</td>
<td>-</td>
</tr>
<tr>
<td>VLAN_OP_TBL_NAME</td>
<td>The name of vlan operation</td>
<td>Up to 16 characters</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
Bind to VPLS instance without vlan tag.

Usage
None

Examples
In the following example, the mpls-vpls command is used to bind an interface to a VPLS instance:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# mpls-vpls vpls1 vlan 100

Related Commands
None

18.3.7 vpls-mac-learning

Command Purpose
Use this command to enable or disable VPLS mac learning with a VPLS instance.

Command Syntax
vpls-mac-learning ( enable | disable )

Command Mode
VPLS Configuration

Default
Enable vpls mac learning with a VPLS instance by default.

Usage
None

Examples
In the following example, the vpls-mac-learning command is used to disable VPLS mac learning with a VPLS instance:
Switch# configure terminal
Switch(config)# mpls vpls vpls1 1
Switch(config-vpls)# vpls-mac-learning disable

Related Commands
None

18.3.8 vpls-mac-limit maximum

Command Purpose
Use this command to set VPLS mac limit maximum

Command Syntax
vpls-mac-limit maximum MAXIMUM
no vpls-mac-limit maximum

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAXIMUM</td>
<td>MAXIMUM value for the VPLS instance</td>
<td>1-4294967295</td>
</tr>
</tbody>
</table>
**Command Mode**
VPLS Configuration

**Default**
VPLS-mac-limit is not enabled by default.

**Usage**
None

**Examples**
In the following example, the vpls-mac-limit command is used to set VPLS mac limit maximum with a VPLS instance:

```
Switch# configure terminal
Switch(config)# mpls vpls vpls1 1
Switch(config-vpls)# vpls-mac-limit maximum 100
```

**Related Commands**
None

---

**18.3.9 clear mpls vpls mac-addresses**

**Command Purpose**
Use this command to remove MAC addresses that have been dynamically learned for faster convergence, and this is accomplished by sending an LDP Withdraw Message to all other PEs over the corresponding LDP session.

**Command Syntax**
```
clear mpls vpls NAME mac-addresses
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>VPLS instance name</td>
<td>Up to 20 characters</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
In the following example, the clear mpls vpls command is used to remove MAC addresses that have been dynamically learned for faster convergence:

```
Switch# clear mpls vpls vpls1 mac-addresses
```

**Related Commands**
None
18.3.10 clear mac address-table vpls

**Command Purpose**
Use this command to remove MAC addresses of Virtual Private Lan Service.

**Command Syntax**
clear mac address-table vpls ( address MAC_ADDR | interface INTERFACE )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC_ADDR</td>
<td>MAC address</td>
<td>MAC address</td>
</tr>
<tr>
<td>INTERFACE</td>
<td>The name of the interface, the format follows below: eth-0-1, agg1, vlan1, etc agg Aggregation interface.agg&lt;1-127&gt; eth Physical interface</td>
<td>Support physical/aggregation ports and eps group</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC

**Default**
None

**Usage**
None

**Examples**
In the following example, the clear mac address-table vpls command is used to remove MAC addresses:
Switch# clear mac address-table vpls peer 1.1.1.1

**Related Commands**
None

18.3.11 show mpls vpls

**Command Purpose**
Use this command to display MPLS VPLS instance information.

**Command Syntax**
show mpls vpls ( NAME | detail | mesh )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Identifying string for VPLS</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>detail</td>
<td>Show detailed VPLS information</td>
<td>-</td>
</tr>
<tr>
<td>mesh</td>
<td>Show MPLS VPLS Mesh Forwarding information</td>
<td>-</td>
</tr>
</tbody>
</table>

**Command Mode**
Privileged EXEC
**Default**
None

**Usage**
None

**Examples**
In the following example, the show mpls vpls command is used to display MPLS VPLS instance information:

```
Switch# show mpls vpls
```

<table>
<thead>
<tr>
<th>Name</th>
<th>VPLS-ID</th>
<th>MPeers(R)</th>
<th>MPeers(T)</th>
<th>SPeers</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1</td>
<td>200</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>Active</td>
</tr>
</tbody>
</table>

In the following example, the show mpls vpls detail command is used to display detailed VPLS information:

```
Switch# show mpls vpls detail
```

Virtual Private LAN Service Instance: v1, ID: 200
Group ID: 0, Configured MTU: NULL
Description: none
AC interface : none
Mesh Peers :
<table>
<thead>
<tr>
<th>Peer</th>
<th>TYPE</th>
<th>State</th>
<th>C-Word</th>
<th>Tunnel name</th>
<th>LSP name</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.3.3</td>
<td>RAW</td>
<td>UP</td>
<td>Disable tun</td>
<td>lsp1</td>
<td></td>
</tr>
</tbody>
</table>

Vpls-mac-learning enable
Vpls-mac-limit maximum 100
Vpls-mac-limit action warn
Discard flooding disabled
Discard unknown-unicast disabled
Discard multicast disabled

In the following example, the show mpls vpls mesh command is used to display MPLS VPLS Mesh Forwarding information:

```
Switch# show mpls vpls mesh
```

<table>
<thead>
<tr>
<th>VPLS-ID</th>
<th>Peer Addr</th>
<th>In-Label</th>
<th>Out-Intf</th>
<th>Out-Label</th>
<th>Type</th>
<th>Lkps/St</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>3.3.3.3</td>
<td>25</td>
<td>eth-0-9</td>
<td>26</td>
<td>RAW</td>
<td>2/Up</td>
</tr>
</tbody>
</table>

**Related Commands**
None

**18.3.12 show mac address-table vpls**

**Command Purpose**
Use this command to display FDB learned by VPLS.
Command Syntax

```
show mac address-table vpls (address MAC_ADDR | interface IFNAME)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC_ADDR</td>
<td>MAC address</td>
<td>MAC address</td>
</tr>
<tr>
<td>IFNAME</td>
<td>The name of the interface, the format follows below: eth-0-1, agg1, vlan1, etc</td>
<td>Support physical/aggregation ports and eps group</td>
</tr>
</tbody>
</table>

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

In the following example, the show mac address-table vpls command is used to display FDB learned by VPLS:

```
Switch# show mac address-table vpls

<table>
<thead>
<tr>
<th>vpls</th>
<th>peer</th>
<th>mac</th>
<th>static</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>eth-0-1</td>
<td>0001.001f.aa12</td>
<td>0</td>
</tr>
<tr>
<td>1000</td>
<td>eth-0-1</td>
<td>407a.a718.3400</td>
<td>0</td>
</tr>
</tbody>
</table>
```

Related Commands

None

18.3.13 mac-address-table

Command Purpose

Use this command on the switch to add static addresses to the MAC address table for a VSI. Use the no form of this command to remove static entries from the table.

Command Syntax

```
mac-address-table MAC-ADDR forward (IFNAME | vpls peer IP_ADDR)
mac-address-table MAC-ADDR discard
mac-address-table MAC-ADDR permit
no mac-address-table MAC-ADDR
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC-ADDR</td>
<td>Destination MAC address (unicast) to add to the address table. Packets with this destination address received in the specified VSI are discarded or forwarded to the specified interface or peer node</td>
<td>MAC address</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Interface to which the received packet is forwarded. Valid interfaces include physical ports and link aggregation ports</td>
<td>Support physical/aggregation ports and eps group</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>IP address of the peer node to which the received packet is forwarded</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>
Command Mode
VPLS Configuration

Default
No static addresses are configured.

Usage
None

Examples
In the following example, the mac-table-address forward command is used to add the static address c2f3.220a.12f4 to the MAC address table. When a packet is received in VPLS v1 with this MAC address as its destination, the packet is forwarded to the specified peer node; the mac-table-address discard command is used to add a MAC blackhole c2f3.220a.12f5 to the MAC address table. When a packet is received in VPLS v1 with this MAC address as its destination, it will be discarded.

Switch(config)# mpls vpls v1 Switch(config-vpls)#

### mac-address-table c2f3.220a.12f4 forward peer 1.1.1.2
### mac-address-table c2f3.220a.12f5 discard

In the following example, the mac-table-address forward command is used to add the static address c2f3.220a.12f4 to the MAC address table. When a packet is received in VPLS v1 with this MAC address as its destination, the packet is forwarded, other packets will be discard:

Switch(config)# configure terminal
Switch(config)# mpls vpls v1
Switch(config-vpls)# mac-address-table c2f3.220a.12f4 forward vpls-peer 1.1.1.2
Switch(config-vpls)# mac-address-table c2f3.220a.12f5 discard

Related Commands
show mac address-table vpls

18.3.14 discard

Command Purpose
Use this command on the switch to set VPLS flood control. Use the no form of this command to unset VPLS flood control.

Command Syntax
discard ( broadcast | unknown-unicast | unknown-multicast )
no discard ( broadcast | unknown-unicast | unknown-multicast )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>broadcast</td>
<td>Broadcast packets</td>
<td>-</td>
</tr>
<tr>
<td>unknown-unicast</td>
<td>Unknown unicast packets</td>
<td>-</td>
</tr>
<tr>
<td>unknown-multicast</td>
<td>Unknown multicast packets</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
VPLS Configuration
Default
Discard flooding is disabled.
Discard unknown-unicast is disabled.
Discard multicast is disabled.

Usage
None

Examples
In the following example, the discard command is used to discard all flooding packets in the VSI:

Switch# configure terminal
Switch(config)# mpls vpls v1
Switch(config-vpls)# discard unknown-unicast

Related Commands
show mpls vpls detail

18.3.15 mpls trust topmost-exp

Command Purpose
Use the exp of the topmost label to map priority and color

Command Syntax
mpls trust topmost-exp
no mpls trust topmost-exp

Command Mode
Global Configuration

Default
None

Usage
None

Examples
In the following example, use the exp of the topmost label:

Switch# configure terminal
Switch(config)# mpls trust topmost-exp

Related Commands

18.3.16 vlan operation table

Command Purpose
Create a vlan operation table
Command Syntax

vlan operation table WORD
no vlan operation table WORD

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>table name</td>
<td>Up to 16 characters</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
None

Examples
In the following example, create a vlan operation table named push:

Switch# configure terminal
Switch(config)# vlan operation table push

Related Commands
rewrite ingress tag

18.3.17 rewrite ingress tag

Command Purpose
Add the edit rule for vlan operation table

Command Syntax
rewrite ingress tag ( push ( vlan VLANID ( second-vlan SVLANID | ) ) | pop ( 1 | 2 ) | translate ( 1-to-1 vlan VLANID | 2-to-1 vlan VLANID | 1-to-2 vlan VLANID second-vlan SVLANID | 2-to-2 vlan VLANID second-vlan SVLANID ) )
no vlan operation

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLANID</td>
<td>Vlan ID</td>
<td>1-4094</td>
</tr>
<tr>
<td>SVLANID</td>
<td>Second Vlan ID</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode
VLAN Operation Configuration

Default
None

Usage
None
Examples
In the following example, add a push rule for a vlan operation table named push, add a vlan tag with vlanid 2 for the ingress packet:

Switch# configure terminal
Switch(config)# vlan operation table push
Switch(config-vlan-operation)# rewrite ingress tag push vlan 2

Related Commands
vlan operation table

18.4 VPWS Commands

18.4.1 mpls l2-circuit

Command Purpose
Use this command to create an instance of MPLS Layer 2 Virtual Circuit.

Command Syntax
mpls l2-circuit NAME VC-ID NEXTHOP ( control-word | ) ( manual | ) ( mtu MTU | ) ( raw | tagged | )
no mpls l2-circuit NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Identifying string for MPLS Layer-2 Virtual Circuit</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>VC-ID</td>
<td>VPWS ID, Identifying value for MPLS Layer-2 Virtual Circuit</td>
<td>1-4294967295</td>
</tr>
<tr>
<td>NEXTHOP</td>
<td>IPv4 Address for end-point for MPLS Layer-2 Virtual Circuit</td>
<td>IPv4 Address</td>
</tr>
<tr>
<td>control-word</td>
<td>Control-word for MPLS Layer-2 Virtual Circuit</td>
<td>-</td>
</tr>
<tr>
<td>manual</td>
<td>Layer-2 Virtual Circuit will created manually</td>
<td>-</td>
</tr>
<tr>
<td>MTU</td>
<td>Layer-2 Virtual Circuit mtu value</td>
<td>576-65535</td>
</tr>
<tr>
<td>raw</td>
<td>PW raw mode</td>
<td>-</td>
</tr>
<tr>
<td>tagged</td>
<td>PW tagged mode</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration

Default
None

Usage
None

Examples
Switch# configure terminal
Switch(config)# mpls l2-circuit pw1 1 100.100.100.1 manual

Related Commands
no mpls l2-circuit
18.4.2 mpls-l2-circuit

Command Purpose
Use this command to bind an interface to a MPLS Layer 2 Virtual Circuit.

Command Syntax
mpls-l2-circuit NAME (ethernet | vlan VLANID | )
no mpls-l2-circuit NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Identifying string for MPLS Layer-2 Virtual Circuit</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>VLANID</td>
<td>Vlan identifier</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

Command Mode
Interface Configuration

Default
PW type is ethernet.

Usage
None

Examples
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# mpls-l2-circuit pw1 vlan 100

Related Commands
no mpls-l2-circuit

18.4.3 mpls l2-circuit-fib-entry

Command Purpose
Use this command to add a Layer 2 Virtual Circuit FIB entry.

Command Syntax
mpls l2-circuit-fib-entry NAME INLABEL OUTLABEL
no mpls l2-circuit-fib-entry NAME

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Identifying string for MPLS Layer-2 Virtual Circuit</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td>INLABEL</td>
<td>Incoming label</td>
<td>16-1048575</td>
</tr>
<tr>
<td>OUTLABEL</td>
<td>Outgoing label</td>
<td>16-1048575</td>
</tr>
</tbody>
</table>

Command Mode
Global Configuration
Default
None

Usage
The MPLS Layer 2 Virtual Circuit should be added use key-word "manual".

Examples
Switch# configure terminal
Switch(config)# mpls l2-circuit-fib-entry pw1 100 200

Related Commands
no mpls l2-circuit-fib-entry

18.4.4 show mpls l2-circuit

Command Purpose
Use this command to show mpls l2 circuit information.

Command Syntax
show mpls l2-circuit { NAME }

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Identifying string for MPLS Layer-2</td>
<td>Up to 20 characters</td>
</tr>
<tr>
<td></td>
<td>Virtual Circuit</td>
<td></td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
Switch# show mpls l2-circuit

<table>
<thead>
<tr>
<th>VC-Name</th>
<th>VC-ID</th>
<th>Interface</th>
<th>AC-type</th>
<th>VLAN</th>
<th>PW-mode</th>
<th>Manual</th>
</tr>
</thead>
<tbody>
<tr>
<td>pw1</td>
<td>100</td>
<td>eth-0-1</td>
<td>Ethernet</td>
<td>N/A</td>
<td>Raw</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Switch# show mpls l2-circuit pw1

MPLS Layer-2 Virtual Circuit: pw1, id: 100
Endpoint: 11.11.3.3
Control Word: 0
MPLS Layer-2 Virtual Circuit Group: none
Bound to interface: eth-0-1
Virtual Circuit Type: Ethernet
Owner: manual
Virtual Circuit is configured as Primary

Related Commands
mpls l2-circuit

18.4.5 show mpls vc-table

Command Purpose
Use this command to show mpls vc forwarding information.

Command Syntax
show mpls vc-table (detail )

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vc-table</td>
<td>MPLS Layer-2 Virtual Circuit table</td>
<td>-</td>
</tr>
<tr>
<td>detail</td>
<td>Show detailed Layer-2 Virtual Circuit information</td>
<td>-</td>
</tr>
</tbody>
</table>

Command Mode
Privileged EXEC

Default
None

Usage
None

Examples
switch# show mpls vc-table

<table>
<thead>
<tr>
<th>VC-ID</th>
<th>PW Intf</th>
<th>AC Intf</th>
<th>L/R Label</th>
<th>Endpoint</th>
<th>Status</th>
<th>Manual</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>eth-0-9</td>
<td>eth-0-1</td>
<td>22/33</td>
<td>11.11.3.3</td>
<td>Active</td>
<td>Yes</td>
</tr>
</tbody>
</table>

mpls l2-circuit: test
ID: 100
Manual: Yes
AC interface: eth-0-9
Peer Address: 3.3.3.3
PW type: Raw
AC type: Ethernet

Related Commands
mpls l2-circuit
https://www.fs.com

All statements, technical information, and recommendations related to the products here are based upon information believed to be reliable or accurate. However, the accuracy or completeness thereof is not guaranteed, and no responsibility is assumed for any inaccuracies. Please contact FS for more information.

Copyright © 2009-2020 FS.COM All Rights Reserved.