MICROSENS

CLI Reference Manual

Ruggedized 19’’ Gigabit Ethernet Switch with 10G Uplink Ports

MICROSENS GmbH & Co. KG
Kueferstr. 16
59067 Hamm/Germany

Tel. +49 2381 9452-0
FAX +49 2381 9452-100
E-Mail info@microsens.de
Web www.microsens.de

Table of Contents

Information available from the MICROSENS Website

Registered users can find the latest firmware versions as well as further information on our web site:

- Registration: www.microsens.de > Partner-Login > Follow the link “Please register here” > Fill in the online registration form and submit it
  - You will receive an email from MICROSENS with a user name and a password
- Login: www.microsens.de > Partner-Login > Enter user name and password > Click the “Login” button
  - Firmware images: Navigate to the device and select the tab “Services”
  - For further information select one of the other tabs

Note:
Make sure the browser allows the execution of scripts.

1. Preface

This CLI Reference Guide describes how to use the CLI and a list of the CLI commands and their arguments regarding the MICROSENS PLR 10G Industrial Switches with the following article no.:

- MS653410MX
- MS653430MX.

The CLI commands described in this document are organized according to feature groups in separate sections.

Note:
The descriptions of commands regarding the following protocols and features apply exclusively to model MS653430MX:

- VRRP (Virtual Router Redundancy Protocol, IPv4)
- Static Routing (IPv4/IPv6)
- RIPv2 (Routing Information Protocol, IPv4)
- OSPFv2, OSPFv3 (Open Shortest Path First, IPv4/IPv6)
- L3 DHCP Relay
- Proxy ARP for IP Routing
- Directed Broadcast
- UDP Relay

Note:
This reference manual may not fully describe all available features, options and parameters of the device you are actually using. Hence this reference manual is kept under constant review and update.

This section describes how to use the CLI. It contains the following topics:

- User (Privilege) Levels
- CLI Command Modes
- Starting the CLI
- CLI Command Conventions
- Interface Naming Conventions
- Entering Commands
- IPv6 Address Conventions
- IP Address and OutOfBand Port
- Upgrading the Firmware

Note:
Due to constant further development the actual scope of CLI commands implemented in the Ruggedized 19” Gigabit Ethernet Switch may differ from the CLI commands mentioned in this reference manual.

1.1. User (Privilege) Levels

Users can be created with one of the following user levels:

- Level 1 - Users with this level can only run **User EXEC mode commands**. Users at this level cannot access the web GUI or commands in the **Privileged EXEC mode**.
- Level 15 - Users with this level can run all commands. Only users at this level can access the web GUI.

A system administrator (user with level 15) can create passwords that allow a level 1 user to temporarily become a level 15 user.

The passwords for each level are set (by an administrator) using the following command:

```
enable password [level privilege-level]{password|encrypted encrypted-password}
```

Using these passwords, you can raise your user level by entering the command `enable` and the password for level 15. The higher level holds only for the current session.

The `disable` command returns the user to a lower level.

To create a user and assign it a user level, use the `username` command. Only users with command level 15, can create users at this level.

Examples

Create passwords for level 15 (by the administrator):

```
switchxxxxxx#configure
switchxxxxxx<conf># enable password level 15 level15@abc
switchxxxxxx<conf>#
```

Create a user with user level 1:

```
switchxxxxxx#configure
switchxxxxxx<conf> username john password john1234 privilege 1
switchxxxxxx<conf>
```

Switch between Level 1 to Level 15. The user must know the password:

```
switchxxxxxx#
switchxxxxxx# enable
Enter Password: ****** (this is the password for level 15 - level15@abc)
switchxxxxxx#
```

If authentication of passwords is performed on RADIUS or TACACS+ servers, the passwords assigned to user level 15 must be configured on the external server and associated with the $enable15$ user names. See the Authentication, Authorization and Accounting (AAA) Commands chapter for details.

1.2. CLI Command Modes

To configure devices, the CLI is divided into various command modes. Each command mode has its own set of specific commands. Entering a question mark ("?") at the console prompt displays a list of commands available for that particular command mode.

A specific command, which varies from mode to mode, is used to navigate from one mode to another. The standard order to access the modes is as follows:

- User EXEC mode
- Privileged EXEC mode
- Global Configuration mode
- Interface Configuration modes.

When starting a session, the initial mode for non-privileged users is the User EXEC mode. Only a limited subset of commands is available in the User EXEC mode. This level is reserved for tasks that do not change the configuration.

Privileged users enter the Privileged EXEC mode directly using a password. This mode provides access to the device Configuration modes.

The modes are described below.

1.2.1. User EXEC Mode

After logging into the device, the user is automatically in User EXEC command mode unless the user is defined as a privileged user. In general, the User EXEC commands enable the user to perform basic tests, and display system information.

The user-level prompt consists of the device "`host name`" followed by the angle bracket (">").

```
console>
```

The default host name is "`console`" unless it has been changed using the `hostname` command in the Global Configuration mode.

1.2.2. Privileged EXEC Mode

Privileged access is password-protected to prevent unauthorized use, because many of the privileged commands set operating system parameters: The password is not displayed on the screen and is case sensitive.

Privileged users enter directly into the Privileged EXEC mode.

Use `disable` to return to the User EXEC mode.

1.2.3. Global Configuration Mode

Global Configuration mode commands apply to features that affect the system as a whole, rather than just a specific interface.

To enter the Global Configuration mode, enter `configure` in the Privileged EXEC mode, and press <**Enter**>.

The Global Configuration mode prompt is displayed.

```
console(config)#
```

Use `exit`, `end` or **Ctrl+z** to return to the Privileged EXEC mode.

1.2.4. Interface Configuration Modes

Commands in the following modes perform specific interface operations:

- **Line Interface** - Contains commands to configure the management connections. These include commands such as line speed, timeout settings, etc. The Global Configuration mode command `line` is used to enter the Line Configuration command mode.
- **VLAN Database -** Contains commands to create a VLAN as a whole. The Global Configuration mode command `vlan database` is used to enter the VLAN Database Interface Configuration mode.
- **Management Access List -** Contains commands to define management access lists. The Global Configuration mode command `management access-list` is used to enter the Management Access List Configuration mode.
- **Port Channel** - Contains commands to configure port channels, for example, assigning ports to a VLAN or port - channel. The Global Configuration mode command `interface port-channel` is used to enter the Port Channel Interface Configuration mode.
- **SSH Public Key-Chain** - Contains commands to manually specify other device SSH public keys. The Global Configuration mode command `crypto key pubkey chain ssh` is used to enter the SSH Public Key chain Configuration mode.

- **Interface** - Contains commands that configure the interface. The Global Configuration mode command `interface` is used to enter the Interface Configuration mode.

1.3. Starting the CLI

The switch can be managed over a direct connection to the switch console port, or via a Telnet connection. The switch is managed by entering command keywords and parameters at the prompt. Using the switch CLI commands is similar to entering commands on a UNIX system.

If access is via a Telnet connection, ensure the device has an IP address defined, corresponding management access is granted, and the workstation used to access the device is connected to the device prior to using CLI commands.

Accessing the CLI from the Console Line

1. Start the device and wait until the startup procedure is complete. The User Exec mode is entered, and the prompt "`console>`" is displayed.
2. Configure the device and enter the necessary commands to complete the required tasks.
3. When finished, exit the session with the `quit` or `exit` command.

Accessing the CLI from Telnet

1. Enter `telnet` and the IP address of the device. A User Name prompt is displayed.
2. Enter the User Name and Password. You are in the Privileged Exec mode.
3. Configure the device and enter the necessary commands to complete the required tasks.
4. When finished, exit the session with the quit or exit command.

When another user is required to log onto the system, the `login` command is entered in the Privileged EXEC command mode. It is possible for up to 5 users to log in at once.

1.4. CLI Command Conventions

The following table describes the command Syntax conventions.

Conventions	Description
[ ]	In a command line, square brackets indicates an optional entry.
{ }	In a command line, curly brackets indicate a selection of compulsory parameters separated by the | character. One option must be selected. For example: **flowcontrol {auto|on|off}** means that for the **flowcontrol** command either **auto**, **on** or **off** must be selected.
Italic font	Indicates a parameter.
<Enter>	Any individual key on the keyboard. For example click <Enter>.
Ctrl+F4	Any combination keys pressed simultaneously on the keyboard.
Screen Display	Indicates system messages and prompts appearing on the console.
all	When a parameter is required to define a range of ports or parameters and **all** is an option, the default for the command is **all** when no parameters are defined. For example, the command

	interface range port-channel has the option of either entering a range of channels, or selecting **all**. When the command is entered without a parameter, it automatically defaults to **all**.
interface-id	This indicates a port, VLAN or LAG. The Syntax for interface_id is as follows: {**port_type**}port-number |{**vlan**} vlan-id | {**port-channel**} LAG-number

1.5. Interface Naming Conventions

Within the CLI, interfaces are denoted by concatenating the following elements:

- **Type of interface -** The following types of interfaces are found on the various types of devices:
- **GigabitEthernet ports (10/100/1000 bits)** -This can be written as either "GigabitEthernet", "gi" or "GE".
- **TenGigabit thernet ports (10000 bits)** - This can be written as either "TenGigabitEthernet", "te" or "xg".
- **LAG (Port Channel) -** This can be written as either "Port-Channel" or "po"**.**
- **VLAN** - This is written as "VLAN"
- **Tunnel -** This is written as "tunnel" or "tu"
- **OOB -** This is written as "OutOfBand" or "oob"
- **Unit Number** - Unit in stack. In standalone models this is always 1 (1 by default)
- **Slot Number** - Always 1
- **Interface Number** - Port, LAG, tunnel or VLAN ID

The syntax for this is:

```
{<ethernet-type>[ ][<unit-number>/]<slot-number>/<port-number>} | {port-channel
| po | ch}[ ]<port-channel-number> | {tunnel | tu}[ ]<tunnel-number> | vlan[ ]
<vlan-id>
```

Sample of these various options are shown in the example below:

```
console(config)#interface GigabitEthernet 1/1/1
console(config)#interface GE 1/1/1
console(config)#interface gi1/1/1
console(config)#interface FastEthernet 1/2/1
console(config)#interface fe1/2/1
console(config)#interface po1
console(config)#interface vlan 1
```

1.5.1. Interface Range

Interfaces may be described on an individual basis or within a range. The interface range command has the following syntax:

```
<interface-range> ::= {<port-type>[ ][<unit-number>/]<slot-number>/<first-port-
number>[ - <last-port-number]} | port-channel[ ]<first-port-channel-number>[ -
<last-port-channel-number>] | tunnel[ ]<first-tunnel-number>[ - <last-tunnel-
number>] | vlan[ ]<first-vlan-id>[ - <last-vlan-id>]
```

A sample of this command is shown in the example below:

```
console#configure
console(config-if)#interface range gi1/1/1-5
```

1.5.2. Interface List

A combination of interface types can be specified in the `interface range` command in the following format:

```
<range-list> ::= <interface-range> | <range-list>, < interface-range>
```
Up to five ranges can be included.

Note:
Range lists can contain either ports and port-channels or VLANs. Combinations of port/port-channels and VLANs are not allowed The space after the comma is optional.

When a range list is defined, a space after the first entry and before the comma (",") must be entered.

A sample of this command is shown in the example below:

```
console#configure
console(config)#interface range gi1/1/1-5 , vlan 1-2
```

1.6. Entering Commands

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters.

E.g. the command `show interfaces status gi1/1/5`:

- `show`, `interfaces` and `status` are keywords,
- `gi` is an argument that specifies the interface type
- `[application-specific]` is an argument that specifies the port.

To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
console(config)#username admin password smith
```

Help information can be displayed in the following ways:

- **Keyword Lookup** - The character "?" is entered in place of a command. A list of all valid commands and corresponding help messages are displayed.
- **Partial Keyword Lookup** - A command is incomplete and the character "?" is entered in place of a parameter. The matched parameters for this command are displayed.

The following describes features that assist in using the CLI:

1.6.1. Terminal Command Buffer

Every time a command is entered in the CLI, it is recorded on an internally managed Command History buffer. Commands stored in the buffer are maintained on a First In First Out (FIFO) basis.These commands can be recalled, reviewed, modified, and reissued. This buffer is not preserved across device resets. The keys that can be used to access the history buffer are described in Table 1.

By default, the history buffer system is enabled, but it can be disabled at any time. For information about the command Syntax to enable or disable the history buffer, see the `history` command.

There is a standard default number of commands that are stored in the buffer. The standard number of 10 commands can be increased to 256. By configuring 0, the effect is the same as disabling the history buffer system. For information about the command Syntax for configuring the command history buffer, see the `history size` command.

To display the history buffer, see `show history` command.

Negating the Effect of Commands

For many configuration commands, the prefix keyword "`no`" can be entered to cancel the effect of a command or reset the configuration to the default value. This guide describes the negation effect for all applicable commands.

Command Completion

If the command entered is incomplete, invalid, or has missing or invalid parameters, an appropriate error message is displayed.

To complete an incomplete command, press the **<Tab>** button. If the characters already entered are not enough for the system to identify a single matching command, press "`?`" to display the available commands matching the characters already entered.

Incorrect or incomplete commands are automatically re-entered next to the cursor. If a parameter must be added, the parameter can be added to the basic command already displayed next to the cursor. The following example indicates that the command interface requires a missing parameter.

```
(config)#interface
%missing mandatory parameter
(config)#interface
```

1.6.2. Keyboard Shortcuts

The CLI has a range of keyboard shortcuts to assist in entering the CLI commands.

The following table describes these shortcuts:

Table 1: Keyboard Keys

Keyboard Key	Description
Up-arrow key	Recalls commands from the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Down-arrow key	Returns the most recent commands from the history buffer after recalling commands with the up arrow key. Repeating the key sequence will recall successively more recent commands.
Ctrl+A	Moves the cursor to the beginning of the command line.

Ctrl+E	Moves the cursor to the end of the command line.
Ctrl+Z / End	Returns back to the Privileged EXEC mode from any mode.
Backspace key	Moves the cursor back one space.
Up-arrow key	Recalls commands from the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.

1.7. Ipv6 Address Conventions

The following describes how to write an IPv6 address, which is a link-local IPv6 address:

The format is: `<ipv6-link-local-address>%<egress-interface>` with `egress-interface` (also known as zone) is `vlan<vlan-id> | po <number> | tunnel <number> | port<number> | 0`.

If the egress interface is not specified, the default interface is selected. Specifying egress interface = 0 is equal to not defining an egress interface.

The following combinations are possible:

- `ipv6_address%egress-interface` - Refers to the IPv6 address on the interface specified.
- `ipv6_address%0` - Refers to the IPv6 address on the single interface on which an IPv6 address is defined.
- `ipv6_address` - Refers to the IPv6 address on the single interface on which an IPv6 address is defined.

1.8. IP Address and OutOfBand Port

The switch supports an IP stack on the OutOfBand (OOB) port. This IP stack is separate from the IP stack running on the ASIC ports, and it has a separate routing table.

If the switch supports more than one IP interface, when you specify a remote IP address or a DNS name, you must also specify the IP stack that is being referred to.

To indicate that the OOB IP stack is being specified, add "`oob/`" before the remote IP address or the DNS name.

The following examples specify the OOB network::

```
ping oob/1.1.1.1
sntp server oob/sntp-server.company.com
permit ip-source 2.2.2.0 mask /24 oob (Management ACL)
```

1.9. Updgrading the Firmware

With firmware versions prior v5.5.3 the device was available in two variants:

- Redundant Ring Protocol RRP (limited to firmware v5.5.1)
- MICROSENS Redundant Ring Protocol MRRP (limited to firmware v5.5.2)

As of firmware v5.5.3 it is possible to use both RRP **or** MRRP (see chapter 53 on page 628). When upgrading to combined firmware v5.5.3 please note the following:

1.9.1. Upgrading from firmware v5.5.1

A firmware upgrade is possible without any adaption or loss of configuration settings. Just download the firmware into the device and start the upgrading process.

1.9.2. Upgrading from firmware v5.5.2

When upgrading to the new combined firmware version v5.5.3, the existing startup config saved on the device may not fit the new combined version (i.e. with MRRP enabled) and should be deleted from the device before the firmware upgrade.

The following upgrade procedure should be performed:

1. Upload the startup config from the device to a PC using the following command:

   `copy startup-config tftp:<address>/<filename.txt>`

   For more information about the command `copy` see section 40.7 on page 474.

2. Delete the startup-config from the device using the following command:

   `delete startup-config`

   For more information about the command `delete` see section 40.8 on page 475.

3. Upgrade the firmware of the device.

4. Force the use of MRRP in the startup-config by adding the following command at the beginning of the startup-config:

   `rrp mode mrrp`

   For more information about the command `rrp mode` see section 53.4 on page 629.

5. Download edited startup-config to the device.

2. 802.1x Commands

2.1. aaa authentication dot1x

To specify which servers are used for authentication when 802.1X authentication is enabled, use `the aaa authentication dot1x` command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- aaa authentication dot1x default {radius | none | {radius none}}
- no aaa authentication dot1x default

Parameters

- radius - Uses the list of all RADIUS servers for authentication
- none - Uses no authentication

Default Configuration

RADIUS server.

Command Mode

Global Configuration mode

User Guidelines

You can select either authentication by a RADIUS server, no authentication (none), or both methods.

If you require that authentication succeeds even if no RADIUS server response was received, specify none as the final method in the command line.

Example

The following example sets the 802.1X authentication mode to RADIUS server authentication. Even if no response was received, authentication succeeds.

```
switchxxxxxx(config)# aaa authentication dot1x default radius none
```

2.2. authentication open

To enable open access (monitoring mode) on this port, use the `authentication open` command in Interface Configuration mode. To disable open access on this port, use the no form of this command.

Syntax

- authentication open
- no authentication open

Parameters

This command has no arguments or keywords.

Default Configuration

Disabled.

Command Mode

Interface (Ethernet, OOB) Configuration mode

User Guidelines

Open Access or Monitoring mode allows clients or devices to gain network access before authentication is performed. In the mode the switch performs failure replies received from a Radius server as success.

Example

The following example enables open mode on interface te1/0/1:

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# authentication open
```

2.3. clear dot1x statistics

To clear 802.1X statistics, use the `clear dot1x statistics` command in Privileged EXEC mode.

Syntax

- clear dot1x statistics [interface-id]

Parameters

- interface-id - Specify an Ethernet port ID.

Default Configuration

Statistics on all ports are cleared.

Command Mode

Privileged EXEC mode

User Guidelines

This command clears all the counters displayed in the show dot1x and show dot1x statistics command.

Example

```
switchxxxxxx# clear dot1x statistics
```

2.4. dot1x authentication

To enable authentication methods on a port, use the `dot1x authentication` command in Interface Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- dot1x authentication [802.1x] [mac] [web]
- no dot1x authentication

Parameters

- 802.1x - Enables authentication based on 802.1X (802.1X-based authentication).
- mac - Enables authentication based on the station's MAC address (MAC-Based authentication).
- web - Enables web-based authentication

Default Configuration

802.1X-Based authentication is enabled.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

The re-authentication interval is 3600 seconds.

Static MAC addresses cannot be authorized by the MAC-based method.

It is not recommended to change a dynamic MAC address to a static one or delete it if the MAC address was authorized by the MAC-based authentication:

- If a dynamic MAC address authenticated by MAC-based authentication is changed to a static one, it will not be manually re-authenticated.
- Removing a dynamic MAC address authenticated by the MAC-based authentication causes its re-authentication.

Example

The following example enables authentication based on 802.1x and the station's MAC address on port te1/0/1:

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# dot1x authentication 802.1x mac
```

2.5. dot1x guest-vlan

To define a guest VLAN, use `the dot1x guest-vlan mode` command in Interface (VLAN) Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- dot1x guest-vlan
- no dot1x guest-vlan

Parameters

N/A

Default Configuration

No VLAN is defined as a guest VLAN.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use the `dot1x guest-vlan enable` command to enable unauthorized users on an interface to access the guest VLAN.

A device can have only one global guest VLAN.

The guest VLAN must be a static VLAN and it cannot be removed.

An unauthorized VLAN cannot be configured as guest VLAN.

Example

The following example defines VLAN 2 as a guest VLAN.

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# dot1x guest-vlan
```

2.6. dot1x guest-vlan enable

To enable unauthorized users on the access interface to the guest VLAN, use the `dot1x guest-vlan enable` command in Interface Configuration mode. To disable access, use the `no` form of this command.

Syntax

- dot1x guest-vlan enable
- no dot1x guest-vlan enable

Parameters

N/A

Default Configuration

The default configuration is disabled.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

This command cannot be configured if the monitoring VLAN is enabled on the interface.

If the port does not belong to the guest VLAN it is added to the guest VLAN as an egress untagged port.

If the authentication mode is single-host or multi-host, the value of PVID is set to the guest VLAN_ID.

If the authentication mode is multi-sessions mode, the PVID is not changed and all untagged traffic and tagged traffic not belonging to the unauthenticated VLANs from unauthorized hosts are mapped to the guest VLAN.

If 802.1X is disabled, the port static configuration is reset.

See the User Guidelines of the `dot1x host-mode` command for more information.

Example

The following example enables unauthorized users on te1/0/1 to access the guest VLAN.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# dot1x guest-vlan enable
```

2.7. dot1x guest-vlan timeout

To set the time delay between enabling 802.1X (or port up) and adding a port to the guest VLAN, use the `dot1x guest-vlan timeout` command in Global Configuration mode. To restore the default configuration, use the `no` form of this command.

Syntax

- dot1x guest-vlan timeout timeout
- no dot1x guest-vlan timeout

Parameters

- timeout - Specifies the time delay in seconds between enabling 802.1X (or port up) and adding the port to the guest VLAN. (Range: 30–180).

Default Configuration

The guest VLAN is applied immediately.

Command Mode

Global Configuration mode

User Guidelines

This command is relevant if the guest VLAN is enabled on the port. Configuring the timeout adds a delay from enabling 802.1X (or port up) to the time the device adds the port to the guest VLAN.

Example

The following example sets the delay between enabling 802.1X and adding a port to a guest VLAN to 60 seconds.

```
switchxxxxxx(config)# dot1x guest-vlan timeout 60
```

2.8. dot1x host-mode

To allow a single host (client) or multiple hosts on an IEEE 802.1X-authorized port, use the `dot1x host-mode` command in Interface Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- dot1x host-mode {multi-host | single-host | multi-sessions}

Parameters

- multi-host - Enable multiple-hosts mode.
- single-host - Enable single-hosts mode.
- multi-sessions - Enable multiple-sessions mode.

Default Configuration

Default mode is multi-host.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

Single-Host Mode

The single-host mode manages the authentication status of the port: the port is authorized if there is an authorized host. In this mode, only a single host can be authorized on the port.

When a port is unauthorized and the guest VLAN is enabled, untagged traffic is remapped to the guest VLAN. Tagged traffic is dropped unless the VLAN tag is the guest VLAN or the unauthenticated VLANs. If guest VLAN is not enabled on the port, only tagged traffic belonging to the unauthenticated VLANs is bridged.

When a port is authorized, untagged and tagged traffic from the authorized host is bridged based on the static vlan membership configured at the port. Traffic from other hosts is dropped.

A user can specify that untagged traffic from the authorized host will be remapped to a VLAN that is assigned by a RADIUS server during the authentication process. In this case, tagged traffic is dropped unless the VLAN tag is the RADIUS-assigned VLAN or the unauthenticated

VLANs. See the `dot1x radius-attributes vlan` command to enable RADIUS VLAN assignment at a port.

The switch removes from FDB all MAC addresses learned on a port when its authentication status is changed from authorized to unauthorized.

Multi-Host Mode

The multi-host mode manages the authentication status of the port: the port is authorized after at least one host is authorized.

When a port is unauthorized and the guest VLAN is enabled, untagged traffic is remapped to the guest VLAN. Tagged traffic is dropped unless the VLAN tag is the guest VLAN or the unauthenticated VLANs. If guest VLAN is not enabled on the port, only tagged traffic belonging to the unauthenticated VLANs is bridged.

When a port is authorized, untagged and tagged traffic from all hosts connected to the port is bridged based on the static vlan membership configured at the port.

A user can specify that untagged traffic from the authorized port will be remapped to a VLAN that is assigned by a RADIUS server during the authentication process. In this case, tagged traffic is dropped unless the VLAN tag is the RADIUS assigned VLAN or the unauthenticated VLANs. See the `dot1x radius-attributes vlan` command to enable RADIUS VLAN assignment at a port.

The switch removes from FDB all MAC addresses learned on a port when its authentication status is changed from authorized to unauthorized.

Multi-Sessions Mode

Unlike the single-host and multi-host modes (port-based modes) the multi-sessions mode manages the authentication status for each host connected to the port (session-based mode). If the multi-sessions mode is configured on a port the port does have any authentication status. Any number of hosts can be authorized on the port. The `dot1x max-hosts` command can limit the maximum number of authorized hosts allowed on the port.

Each authorized client requires a TCAM rule. If there is no available space in the TCAM, the authentication is rejected.

When using the dot1x host-mode command to change the port mode to single-host or multi-host when authentication is enabled, the port state is set to unauthorized.

If the dot1x host-mode command changes the port mode to multi-session when authentication is enabled, the state of all attached hosts is set to unauthorized.

To change the port mode to single-host or multi-host, set the port (dot1x port-control) to force-unauthorized, change the port mode to single-host or multi-host, and set the port to authorization auto.

multi-sessions mode cannot be configured on the same interface together with Policy Based VLANs configured by the following commands:

- switchport general map protocol-group vlans
- switchport general map macs-group vlans

Tagged traffic belonging to the unauthenticated VLANs is always bridged regardless if a host is authorized or not.

When the guest VLAN is enabled, untagged and tagged traffic from unauthorized hosts not belonging to the unauthenticated VLANs is bridged via the guest VLAN.

Traffic from an authorized hosts is bridged in accordance with the port static configuration. A user can specify that untagged and tagged traffic from the authorized host not belonging to the unauthenticated VLANs will be remapped to a VLAN that is assigned by a RADIUS server during the authentication process. See the `dot1x radius-attributes vlan` command to enable RADIUS VLAN assignment at a port.

The switch does not remove from FDB the host MAC address learned on the port when its authentication status is changed from authorized to unauthorized. The MAC address will be removed after the aging timeout expires.

Example

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# dot1x host-mode multi-host
```

2.9. dot1x max-hosts

To configure the maximum number of authorized hosts allowed on the interface, use the `dot1x max-hosts` command in Interface Configuration mode. To restore the default configuration, use the `no` form of this command.

Syntax

- dot1x max-hosts count
- no dot1x max-hosts

Parameters

- count - Specifies the maximum number of authorized hosts allowed on the interface. May be any 32 bits positive number.

Default Configuration

No limitation.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

By default, the number of authorized hosts allowed on an interface is not limited. To limit the number of authorized hosts allowed on an interface, use the `dot1x max-hosts` command.

This command is relevant only for multi-session mode.

Example

The following example limits the maximum number of authorized hosts on Ethernet port te1/0/1 to 6:

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# dot1x max-hosts 6
```

2.10. dot1x max-req

To set the maximum number of times that the device sends an Extensible Authentication Protocol (EAP) request/identity frame (assuming that no response is received) to the client before restarting the authentication process, use the `dot1x max-req` command in Interface Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- dot1x max-req count
- no dot1x max-req

Parameters

- count - Specifies the maximum number of times that the device sends an EAP request/identity frame before restarting the authentication process. (Range: 1–10).

Default Configuration

The default maximum number of attempts is 2.

Command Mode

Interface (Ethernet, OOB) Configuration mode

User Guidelines

The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Example

The following example sets the maximum number of times that the device sends an EAP request/identity frame to 6.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# dot1x max-req 6
```

2.11. dot1x port-control

To enable manual control of the port authorization state, use the `dot1x port-control` command in Interface Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- dot1x port-control {auto | force-authorized | force-unauthorized}
- no dot1x port-control

Parameters

- auto - Enables 802.1X authentication on the port and causes it to transition to the authorized or unauthorized state, based on the 802.1X authentication exchange between the device and the client.
- force-authorized - Disables 802.1X authentication on the interface and causes the port to transition to the authorized state without any authentication exchange required. The port sends and receives traffic without 802.1X-based client authentication.
- force-unauthorized - Denies all access through this port by forcing it to transition to the unauthorized state and ignoring all attempts by the client to authenticate. The device cannot provide authentication services to the client through this port.

Default Configuration

The port is in the force-authorized state.

Command Mode

Interface (Ethernet, OOB) Configuration mode

User Guidelines

The switch removes all MAC addresses learned on a port when its authorization control is changed from force-authorized to another.

Note. It is recommended to disable spanning tree or to enable spanning-tree PortFast mode on 802.1X edge ports in auto state that are connected to end stations, in order to proceed to the forwarding state immediately after successful authentication.

Example

The following example sets 802.1X authentication on te1/0/1 to auto mode.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# dot1x port-control auto
```

2.12. dot1x radius-attributes vlan

To enable RADIUS-based VLAN assignment, use the `dot1x radius-attributes vlan` command in Interface Configuration mode. To disable RADIUS-based VLAN assignment, use the no form of this command.

Syntax

- dot1x radius-attributes vlan [reject | static]
- no dot1x radius-attributes vlan

Parameters

- reject - If the RADIUS server authorized the supplicant, but did not provide a supplicant VLAN the supplicant is rejected. If the parameter is omitted, this option is applied by default.
- static - If the RADIUS server authorized the supplicant, but did not provide a supplicant VLAN, the supplicant is accepted.

Default Configuration

reject

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

If RADIUS provides invalid VLAN information, the authentication is rejected.

If a RADIUS server assigns a client with a non-existing VLAN, the switch creates the VLAN. The VLAN is removed when it is no longer being used.

If RADIUS provides valid VLAN information and the port does not belong to the VLAN received from RADIUS, it is added to the VLAN as an egress untagged port. When the last authorized client assigned to the VLAN becomes unauthorized or 802.1x is disabled on the port, the port is excluded from the VLAN.

If the authentication mode is single-host or multi-host, the value of PVID is set to the VLAN_ID.

If an authorized port in the single-host or multi-host mode changes its status to unauthorized, the port static configuration is reset.

If the authentication mode is multi-sessions mode, the PVID is not changed and all untagged traffic and tagged traffic not belonging to the unauthenticated VLANs are mapped to the VLAN using TCAM.

If the last authorized host assigned to a VLAN received from RADIUS connected to a port in the multi-sessions mode changes its status to unauthorized, the port is removed from the VLAN if it is not in the static configuration.

See the User Guidelines of the `dot1x host-mode` command for more information.

If 802.1X is disabled the port static configuration is reset.

If the reject keyword is configured and the RADIUS server authorizes the host but the RADIUS accept message does not assign a VLAN to the supplicant, authentication is rejected.

If the static keyword is configured and the RADIUS server authorizes the host then even though the RADIUS accept message does not assign a VLAN to the supplicant, authentication is accepted and the traffic from the host is bridged in accordance with port static configuration.

If this command is used when there are authorized ports/hosts, it takes effect at subsequent authentications. To manually re-authenticate, use the `dot1x re-authenticate` command.

The command cannot be configured on the OOB port.

The command cannot be configured on a port if it together with

- Multicast TV-VLAN
- Q-in-Q
- Voice VLAN

Examples

Example 1. This example enables user-based VLAN assignment. If the RADIUS server authorized the supplicant, but did not provide a supplicant VLAN, the supplicant is rejected.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# dot1x radius-attributes vlan
switchxxxxxx(config-if)# exit
```

Example 2. This example enables user-based VLAN assignment. If the RADIUS server authorized the supplicant but did not provide a supplicant VLAN, the supplicant is accepted and the static VLAN configurations is used.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# dot1x radius-attributes staticswitchxxxxxx(config-if)#
exit
```

2.13. dot1x re-authenticate

To initiate manually re-authentication of all 802.1X-enabled ports or the specified 802.1X-enabled port, use the `dot1x re-authenticate` command in Privileged EXEC mode.

Syntax

- dot1x re-authenticate [interface-id]

Parameters

- interface-id - Specifies an Ethernet port or OOB port.

Default Configuration

If no port is specified, command is applied to all ports.

Command Mode

Privileged EXEC mode

Example

The following command manually initiates re-authentication of 802.1X-enabled te1/0/1:

```
switchxxxxxx# dot1x re-authenticate te1/0/1
```

2.14. dot1x reauthentication

To enable periodic re-authentication of the client, use the `dot1x reauthentication` command in Interface Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- dot1x reauthentication
- no dot1x reauthentication

Parameters

N/A

Default Configuration

Periodic re-authentication is disabled.

Command Mode

Interface (Ethernet, OOB) Configuration mode

User Guide

The automatic re-authentication interval is 3600 seconds.

Example

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# dot1x reauthentication
```

2.15. dot1x system-auth-control

To enable 802.1X globally, use the `dot1x system-auth-control` command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- dot1x system-auth-control
- no dot1x system-auth-control

Parameters

N/A

Default Configuration

Disabled.

Command Mode

Global Configuration mode

Example

The following example enables 802.1X globally.

```
switchxxxxxx(config)# dot1x system-auth-control
```

2.16. dot1x timeout quiet-period

To set the time interval that the device remains in a quiet state following a failed authentication exchange, use the `dot1x timeout quiet-period` command in Interface Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- dot1x timeout quiet-period seconds
- no dot1x timeout quiet-period

Parameters

- seconds - Specifies the time interval in seconds that the device remains in a quiet state following a failed authentication exchange with a client. (Range: 10–65535 seconds).

Default Configuration

The default quiet period is 60 seconds.

Command Mode

Interface (Ethernet, OOB) Configuration mode

User Guidelines

During the quiet period, the device does not accept or initiate authentication requests.

The default value of this command should only be changed to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

To provide faster response time to the user, a smaller number than the default value should be entered.

For 802.1x and MAC-based authentication, the number of failed logins is 1.

For 802.1x-based and MAC-based authentication methods, the quite period is applied after each failed attempt.

Example

The following example sets the time interval that the device remains in the quiet state following a failed authentication exchange to 120 seconds.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# dot1x timeout quiet-period 120
```

2.17. dot1x timeout reauth-period

To set the number of seconds between re-authentication attempts, use the `dot1x timeout reauth-period` command in Interface Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- dot1x timeout reauth-period seconds
- no dot1x timeout reauth-period

Parameters

- reauth-period seconds - Number of seconds between re-authentication attempts. (Range: 300-4294967295).

Default Configuration

3600

Command Mode

Interface (Ethernet, OOB) Configuration mode

User Guidelines

The command is only applied to the 802.1x authentication method.

Example

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# dot1x timeout reauth-period 5000
```

2.18. dot1x timeout server-timeout

To set the time interval during which the device waits for a response from the authentication server, use the `dot1x timeout server-timeout` command in Interface Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- dot1x timeout server-timeout seconds
- no dot1x timeout server-timeout

Parameters

- server-timeout seconds - Specifies the time interval in seconds during which the device waits for a response from the authentication server. (Range: 1–65535 seconds).

Default Configuration

The default timeout period is 30 seconds.

Command Mode

Interface (Ethernet, OOB) Configuration mode

User Guidelines

The actual timeout period can be determined by comparing the value specified by this command to the result of multiplying the number of retries specified by the `radius-server retransmit` command by the timeout period specified by the `radius-server retransmit` command, and selecting the lower of the two values.

Example

The following example sets the time interval between retransmission of packets to the authentication server to 3600 seconds.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# dot1x timeout server-timeout 3600
```

2.19. dot1x timeout supp-timeout

To set the time interval during which the device waits for a response to an Extensible Authentication Protocol (EAP) request frame from the client before resending the request, use the `dot1x timeout supp-timeout` command in Interface Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- dot1x timeout supp-timeout seconds
- no dot1x timeout supp-timeout

Parameters

- supp-timeout seconds - Specifies the time interval in seconds during which the device waits for a response to an EAP request frame from the client before resending the request. (Range: 1–65535 seconds).

Default Configuration

The default timeout period is 30 seconds.

Command Mode

Interface (Ethernet, OOB) Configuration mode

User Guidelines

The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

The command is only applied to the 802.1x authentication method.

Example

The following example sets the time interval during which the device waits for a response to an EAP request frame from the client before resending the request to 3600 seconds.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# dot1x timeout supp-timeout 3600
```

2.20. dot1x timeout tx-period

To set the time interval during which the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the client before resending the request, use the `dot1x timeout tx-period` command in Interface Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- dot1x timeout tx-period seconds
- no dot1x timeout tx-period

Parameters

- seconds - Specifies the time interval in seconds during which the device waits for a response to an EAP-request/identity frame from the client before resending the request. (Range: 30–65535 seconds).

Default Configuration

The default timeout period is 30 seconds.

Command Mode

Interface (Ethernet, OOB) Configuration mode

User Guidelines

The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

The command is only applied to the 802.1x authentication method.

Example

The following command sets the time interval during which the device waits for a response to an EAP request/identity frame to 60 seconds.

```
switchxxxxxx(config)# interface te1/0/1:
switchxxxxxx(config-if)# dot1x timeout tx-period 60
```

2.21. dot1x traps authentication failure

To enable sending traps when an 802.1X authentication method failed, use the `dot1x traps authentication failure` command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- dot1x traps authentication failure {[802.1x] [mac] [web]}
- no dot1x traps authentication failure

Parameters

- 802.1x - Enables traps for 802.1X-based authentication.
- mac - Enables traps for MAC-based authentication.
- web - Enables traps for web-based authentication.

Default Configuration

All traps are disabled.

Command Mode

Global Configuration mode

User Guidelines

Any combination of the keywords are allowed. At least one keyword must be configured.

A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.

Example

The following example enables sending traps when a MAC address fails to be authorized by the 802.1X mac-authentication access control.

```
switchxxxxxx(config)# dot1x traps authentication failure 802.1x
```

2.22. dot1x traps authentication quiet

To enable sending traps when a host state is set to the quiet state after failing the maximum sequential attempts of login, use the `dot1x traps authentication quiet` command in Global Configuration mode. To disable the traps, use the no form of this command.

Syntax

- dot1x traps authentication quiet
- no dot1x traps authentication quiet

Parameters

N/A

Default Configuration

Quiet traps are disabled.

Command Mode

Global Configuration mode

User Guidelines

The traps are sent after the client is set to the quiet state after the maximum sequential attempts of login.

The command is only applied to the web-based authentication.

A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.

Example

The following example enables sending traps when a host is set in the quiet state:

```
switchxxxxxx(config)# dot1x traps authentication quiet
```

2.23. dot1x traps authentication success

To enable sending traps when a host is successfully authorized by an 802.1X authentication method, use the `dot1x traps authentication success` command in Global Configuration mode. To disable the traps, use the no form of this command.

Syntax

- dot1x traps authentication success {[802.1x] [mac] [web]}
- no dot1x traps authentication success

Parameters

- 802.1x - Enables traps for 802.1X-based authentication.
- mac - Enables traps for MAC-based authentication.
- web- Enables traps for web-based authentication.

Default Configuration

Success traps are disabled.

Command Mode

Global Configuration mode

User Guidelines

Any combination of the keywords are allowed. At least one keyword must be configured.

A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.

Example

The following example enables sending traps when a MAC address is successfully authorized by the 802.1X MAC-authentication access control.

```
switchxxxxxx(config)# dot1x traps authentication success mac
```

2.24. dot1x unlock client

To unlock a locked (in the quiet period) client, use the `dot1x unlock client` command in Privileged EXEC mode.

Syntax

- dot1x unlock client interface-id mac-address

Parameters

- interface-id - Interface ID where the client is connected to.
- mac-address - Client MAC address.

Default Configuration

The client is locked until the silence interval is over.

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to unlock a client that was locked after the maximum allowed authentication failed attempts and to end the quiet period. If the client is not in the quiet period, the command has no affect.

Example

```
switchxxxxxx# dot1x unlock client te1/0/1 00:01:12:af:00:56
```

2.25. dot1x violation-mode

To configure the action to be taken when an unauthorized host on authorized port in single-host mode attempts to access the interface, use the `dot1x violation-mode` command in Interface Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- dot1x violation-mode {restrict | protect | shutdown}

- no dot1x violation-mode

Parameters

- restrict - Generates a trap when a station, whose MAC address is not the supplicant MAC address, attempts to access the interface. The minimum time between the traps is 1 second. Those frames are forwarded but their source addresses are not learned.
- protect - Discard frames with source addresses that are not the supplicant address.
- shutdown - Discard frames with source addresses that are not the supplicant address and shutdown the port.

Default Configuration

Protect

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

The command is relevant only for single-host mode.

For BPDU messages whose MAC addresses are not the supplicant MAC address are not discarded in Protect mode.

BPDU message whose MAC addresses are not the supplicant MAC address cause a shutdown in Shutdown mode.

Example

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# dot1x violation-mode protect
```

2.26. show dot1x

To display the 802.1X interfaces or specified interface status, use the `show dot1x` command in Privileged EXEC mode.

Syntax

- show dot1x [interface interface-id | detailed]

Parameters

- interface interface-id - Specify an interface ID. The interface ID must be an Ethernet port.
- detailed - Displays information even for non-present ports in addition to present ports.

Default Configuration

Display for all ports. If detailed is not used, only present ports are displayed.

If the MAC-Based password is configured the `dot1x mac-auth password` command, its MD5 checksum is displayed, else the `Username` word is displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays authentication information for all interfaces on which 802.1x is enabled:

```
switchxxxxxx# show dot1x
Authentication is enabled
Authenticating Servers: Radius, None
Guest VLAN: VLAN 11, timeout 30 sec
Authentication failure traps are enabled for 802.1x+mac
Authentication success traps are enabled for 802.1x Authentication quiet traps
are enabled for 802.1x
te1/0/1
 Host mode: multi-sessions
 Authentication methods: 802.1x+mac
 Port Adminstrated status: auto
 Guest VLAN: enabled
 VLAN Radius Attribute: enabled, static
 Open access: disabled
 Server-timeout: 30 sec
 Maximum Hosts: unlimited
 Maximum Login Attempts: 3
 Reauthentication is enabled
 Reauthentication period: 3600 sec
 Quiet Period: 60 sec
 Interfaces 802.1X-Based Parameters
 Tx period: 30 sec
 Supplicant timeout: 30 sec
 max-req: 2
 Authentication success: 9
 Authentication fails: 1
 Number of Authorized Hosts: 10
te1/0/2
 Host mode: single-host
 Authentication methods: 802.1x+mac
 Port Adminstrated status: auto
 Port Operational status: authorized
 Guest VLAN: disabled
 VLAN Radius Attribute: enabled
 Open access: enabled
 Server-timeout: 30 sec
 Aplied Authenticating Server: Radius
 Applied Authentication method: 802.1x
 Session Time (HH:MM:SS): 00:25:22
 MAC Address: 00:08:78:32:98:66
 Username: Bob
 Violation Mode: restrict
 Trap: enabled
 Trap Min Interval: 20 sec
 Violations were detected: 9
 Reauthentication is enabled
 Reauthentication period: 3600 sec
 Silence period: 1800 sec
 Quiet Period: 60 sec
 Interfaces 802.1X-Based Parameters
 Tx period: 30 sec Supplicant timeout: 30 sec
 max-req: 2
 Authentication success: 2 Authentication fails: 0
te1/0/3
 Host mode: multi-host
 Authentication methods: 802.1x+mac
```

```
Port Adminstrated status: auto
Port Operational status: authorized
Guest VLAN: disabled
VLAN Radius Attribute: disabled
Open access: disabled
Server-timeout: 30 sec
Aplied Authenticating Server: Radius
Applied Authentication method: 802.1x
Session Time (HH:MM:SS): 00:25:22
MAC Address: 00:08:78:32:98:66
Username: Bob
Violation Mode: restrict
Trap: enabled
Trap Min Interval: 20 sec
Violations were detected: 0
Reauthentication is enabled
Reauthentication period: 3600 sec
Silence period: 1800 sec
Quiet Period: 60 sec
Interfaces 802.1X-Based Parameters
Tx period: 30 sec
Supplicant timeout: 30 sec
max-req: 2
Authentication success: 20
Authentication fails: 0
Host mode: multi-host
Authentication methods: 802.1x+mac
Port Adminstrated status: force-auto
Guest VLAN: disabled
VLAN Radius Attribute: disabled
Open access: disabled
Server-timeout: 30 sec
Aplied Authenticating Server: Radius
Applied Authentication method: 802.1x
Session Time (HH:MM:SS): 00:25:22
MAC Address: 00:08:78:32:98:66
Username: Bob
Violation Mode: restrict
Trap: enabled
Trap Min Interval: 20 sec
Violations were detected: 0
Reauthentication is enabled
Reauthentication period: 3600 sec
Silence period: 1800 sec
Quiet Period: 60 sec
Interfaces 802.1X-Based Parameters
Tx period: 30 sec
Supplicant timeout: 30 sec max-req: 2
Authentication success: 0
Authentication fails: 0
Supplicant Configuration:
retry-max: 2
EAP time period: 15 sec
Supplicant Held Period: 30 sec
Credentials Name: Basic-User
Supplicant Operational status: authorized
```

The following describes the significant fields shown in the display:

- Port - The port interface-id.
- Host mode - The port authentication configured mode. Possible values: single-host, multi-host, multi-sessions.
  - single-host
  - multi-host
  - multi-sessions
- Authentication methods - Authentication methods configured on port. Possible values are combinations of the following methods:
  - 802.1x
  - mac
- Port Administrated status - The port administration (configured) mode. Possible values: force-auth, force-unauth, auto.
- Port Operational status - The port operational (actual) mode. Possible values: authorized or unauthorized.
- Username - Username representing the supplicant identity. This field shows the username if the port control is auto. If the port is Authorized, it displays the username of the current user. If the port is Unauthorized, it displays the last user authorized successfully.
- Quiet period - Number of seconds that the device remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password).
- Silence period - Number of seconds that If an authorized client does not send traffic during the silence period specified by the command, the state of the client is changed to unauthorized.
- Tx period - Number of seconds that the device waits for a response to an Extensible

Authentication Protocol (EAP) request/identity frame from the client before resending the request.

- Max req - Maximum number of times that the device sends an EAP request frame (assuming that no response is received) to the client before restarting the authentication process.
- Server timeout - Number of seconds that the device waits for a response from the authentication server before resending the request.
- Session Time - Amount of time (HH:MM:SS) that the user is logged in.
- MAC address - Supplicant MAC address.
- Authentication success - Number of times the state machine received a Success message from the Authentication Server.Authentication fails - Number of times the state machine received a Failure message from the Authentication Server.

2.27. show dot1x locked clients

To display all clients who are locked and in the quiet period, use the `show dot1x locked clients` command in Privileged EXEC mode.

Syntax

- show dot1x locked clients

Parameters

N/A

Command Mode

Privileged EXEC mode

User Guidelines

Use the `show dot1x locked clients` command to display all locked (in the quiet period) clients.

Examples

The following example displays locked clients:

```
switchxxxxxx# show dot1x locked clients
Port MAC Address Remaining Time
------ ------------- --------------
te1/0/1 0008.3b79.8787 20
te1/0/1 0008.3b89.3128 40
te1/0/2 0008.3b89.3129 10
```

2.28. show dot1x statistics

To display 802.1X statistics for the specified port, use the `show dot1x statistics` command in Privileged EXEC mode.

Syntax

- show dot1x statistics interface interface-id

Parameters

- interface interface-id - Specifies an Ethernet port or OOB port.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays 802.1X statistics for te1/0/1.

```
switchxxxxxx# show dot1x statistics interface te1/0/1
EapolFramesRx: 11 EapolFramesTx: 12
EapolStartFramesRx: 1
EapolLogoffFramesRx: 1
EapolRespIdFramesRx: 3
EapolRespFramesRx: 6
EapolReqIdFramesTx: 3
EapolReqFramesTx: 6
InvalidEapolFramesRx: 0
EapLengthErrorFramesRx: 0
LastEapolFrameVersion: 1
LastEapolFrameSource: 00:08:78:32:98:78
```

The following table describes the significant fields shown in the display:

Field	Description

EapolFramesRx	Number of valid EAPOL frames of any type that have been received by this Authenticator.
EapolFramesTx	Number of EAPOL frames of any type that have been transmitted by this Authenticator.
EapolStartFramesRx	Number of EAPOL Start frames that have been received by this Authenticator.
EapolLogoffFramesRx	Number of EAPOL Logoff frames that have been received by this Authenticator.
EapolRespIdFramesRx	Number of EAP Resp/Id frames that have been received by this Authenticator.
EapolRespFramesRx	Number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
EapolReqIdFramesTx	Number of EAP Req/Id frames that have been transmitted by this Authenticator.
EapolReqFramesTx	Number of EAP Request frames (other than Req/Id frames) that have been transmitted by this Authenticator.
InvalidEapolFramesRx	Number of EAPOL frames that have been received by this Authenticator for which the frame type is not recognized.
EapLengthErrorFramesRx	Number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
LastEapolFrameVersion	Protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	Source MAC address carried in the most recently received EAPOL frame.

2.29. show dot1x users

To display active 802.1X authorized users for the device, use the `show dot1x users` command in Privileged EXEC mode.

Syntax

- show dot1x users [username username]

Parameters

- username username - Specifies the supplicant username (Length: 1–160 characters).

Default Configuration

Display all users.

Command Mode

Privileged EXEC mode

Examples

Example 1. The following commands displays all 802.1x users:

```
show dot1x users
Port Username MAC Address Auth Auth Session Time VLAN
  Method Server
-------------------------------------------------------------------
te1/0/1 Bob 0008.3b71.1111 802.1x Remote 09:01:00 1020
te1/0/2 Allan 0008.3b79.8787 802.1x Remote 00:11:12
te1/0/2 John 0008.3baa.0022 802.1x Remote 00:27:16
```

Example 2. The following example displays 802.1X user with supplicant username Bob:

```
switchxxxxxx# show dot1x users username Bob
Port Username MAC Address Auth Auth Session Time VLAN
  Method Server
-------------------------------------------------------------------
te1/0/1 Bob 0008.3b71.1111 802.1x Remote 09:01:00 1020
```

3. Authentication, Authorization and Accounting (AAA) Commands

3.1. aaa authentication login

Use the `aaa authentication login` in command in Global Configuration mode to set one or more authentication methods to be applied during login. Use the no form of this command to restore the default authentication method.

Syntax

- aaa authentication login {default | list-name} method1 [method2...]
- no aaa authentication login {default | list-name}

Parameters

- default - Uses the authentication methods that follow this argument as the default method list when a user logs in (this list is unnamed).
- list-name - Specifies a name of a list of authentication methods activated when a user logs in. (Length: 1–12 characters)
- method1 [method2...] - Specifies a list of methods that the authentication algorithm tries (in the given sequence). Each additional authentication method is used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify none as the final method in the command line. Select one or more methods from the following list::

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
local	Uses the locally-defined usernames for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

If no methods are specified, the default are the locally-defined users and passwords. This is the same as entering the command aaa authentication login local.

Command Mode

Global Configuration mode

User Guidelines

Create a list of authentication methods by entering this command with the list-name parameter where list-name is any character string. The method arguments identifies the list of methods that the authentication algorithm tries, in the given sequence.

The default and list names created with this command are used with the `login authentication` command.

The no aaa authentication login list-name command deletes a list-name only if it has not been referenced by another command.

Example

The following example sets the authentication login methods for the console.

```
switchxxxxxx(config)# aaa authentication login authen-list radius local none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# login authentication authen-list
```

3.2. aaa authentication enable

The `aaa authentication enable` command in Global Configuration mode sets one or more authentication methods for accessing higher privilege levels. To restore the default authentication method, use the no form of this command.

Syntax

- aaa authentication enable {default | list-name} method [method2...]}
- no aaa authentication enable {default | list-name}

Parameters

- default - Uses the listed authentication methods that follow this argument as the default method list, when accessing higher privilege levels.
- list-name - Specifies a name for the list of authentication methods activated when a user accesses higher privilege levels. (Length: 1–12 characters)
- method [method2...] - Specifies a list of methods that the authentication algorithm tries, in the given sequence. The additional authentication methods are used only if the previous method returns an error, not if it fails. Specify none as the final method in the command line to ensure that the authentication succeeds, even if all methods return an error. Select one or more methods from the following list:

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

The enable password command defines the default authentication login method. This is the same as entering the command aaa authentication enable default enable.

On a console, the enable password is used if a password exists. If no password is set, authentication still succeeds. This is the same as entering the command aaa authentication enable default enable none.

Command Mode

Global Configuration mode

User Guidelines

Create a list by entering the aaa authentication enable list-name method1 [method2...] command where list-name is any character string used to name this list. The method argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

The default and list names created by this command are used with the `enable authentication` command.

All aaa authentication enable requests sent by the device to a RADIUS server include the username $enabx$., where x is the requested privilege level.

All aaa authentication enable requests sent by the device to a TACACS+ server include the username that is entered for login authentication.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. Specify none as the final method in the command line to ensure that the authentication succeeds even if all methods return an error.

`no aaa authentication enable list-name` deletes list-name if it has not been referenced.

Example

The following example sets the enable password for authentication for accessing higher privilege levels.

```
switchxxxxxx(config)# aaa authentication enable enable-list radius none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# enable authentication enable-list
```

3.3. login authentication

The `login authentication` Line Configuration mode command specifies the login authentication method list for a remote Telnet or console session. Use the no form of this command to restore the default authentication method.

Syntax

- login authentication {default | list-name}
- no login authentication

Parameters

- default - Uses the default list created with the aaa authentication login command.
- list-name - Uses the specified list created with the aaa authentication login command.

Default Configuration

default

Command Mode

Line Configuration Mode

Examples

Example 1 - The following example specifies the login authentication method as the default method for a console session.

```
switchxxxxxx(config)# line console
```

```
switchxxxxxx(config-line)# login authentication default
```

Example

Example 2 - The following example sets the authentication login methods for the console as a list of methods.

```
switchxxxxxx(config)# aaa authentication login authen-list radius local none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# login authentication authen-list
```

3.4. enable authentication

The `enable authentication` Line Configuration mode command specifies the authentication method for accessing a higher privilege level from a remote Telnet or console. Use the no form of this command to restore the default authentication method.

Syntax

- enable authentication {default | list-name}
- no enable authentication

Parameters

- default - Uses the default list created with the aaa authentication enable command.
- list-name - Uses the specified list created with the aaa authentication enable command.

Default Configuration

default

Command Mode

Line Configuration Mode

Examples

Example 1 - The following example specifies the authentication method as the default method when accessing a higher privilege level from a console.

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# enable authentication default
```

Example 2 - The following example sets a list of authentication methods for accessing higher privilege levels.

```
switchxxxxxx(config)# aaa authentication enable enable-list radius none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# enable authentication enable-list
```

3.5. ip http authentication

The `ip http authentication` Global Configuration mode command specifies authentication methods for HTTP server access. Use the no form of this command to restore the default authentication method.

Syntax

- ip http authentication aaa login-authentication method1 [method2...]
- no ip http authentication aaa login-authentication

Parameters

- method [method2...] - Specifies a list of methods that the authentication algorithm tries, in the given sequence. The additional authentication methods are used only if the previous method returns an error, not if it fails. Specify none as the final method in the command line to ensure that the authentication succeeds, even if all methods return an error. Select one or more methods from the following list:

Keyword	Description
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

The local user database is the default authentication login method. This is the same as entering the ip http authentication local command.

Command Mode

Global Configuration mode

User Guidelines

The command is relevant for HTTP and HTTPS server users.

Example

The following example specifies the HTTP access authentication methods.

```
switchxxxxxx(config)# ip http authentication aaa login-authentication radius
local none
```

3.6. show authentication methods

The `show authentication methods` Privileged EXEC mode command displays information about the authentication methods.

Syntax

- show authentication methods

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays the authentication configuration:

```
switchxxxxxx# show
```

```
authentication methods Login Authentication Method Lists
--------------------------------
Default: Radius, Local, Line
Console_Login: Line, None
Enable Authentication Method Lists
--------------------------------
Default: Radius, Enable
Console_Enable(with authorization): Enable, None

      Line              Login Method List    Enable Method List
      --------------    -----------------    ------------------
      Console           Console_Login        Console_Enable
      Telnet            Default              Default
      SSH               Default              Default
HTTP, HHTPS: Radius, local
Dot1x: Radius
```

3.7. password

Use the `password` Line Configuration mode command to specify a password on a line (also known as an access method, such as a console or Telnet). Use the no form of this command to return to the default password.

Syntax

- password password [encrypted]
- no password

Parameters

- password - Specifies the password for this line. (Length: 0–159 characters)
- encrypted - Specifies that the password is encrypted and copied from another device configuration.

Default Configuration

No password is defined.

Command Mode

Line Configuration Mode

Example

The following example specifies the password ‘secret’ on a console.

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# password secret
```

3.8. enable password

Use the `enable password` Global Configuration mode command to set a local password to control access to normal and privilege levels. Use the no form of this command to return to the default password.

Syntax

- enable password [level privilege-level] {unencrypted-password | encrypted |encrypted-password}
- no enable password [level level]

Parameters

- level privilege-level - Level for which the password applies. If not specified, the level is 15. (Range: 1–15)
- unencrypted-password - Password for this level. (Range: 0–159 chars)
- password encrypted encrypted-password - Specifies that the password is encrypted. Use this keyword to enter a password that is already encrypted (for instance that you copied from another the configuration file of another device). (Range: 1–40)

Default Configuration

Default for level is 15.

Passwords are encrypted by default.

Command Mode

Global Configuration mode

User Guidelines

When the administrator configures a new enable password, this password is encrypted automatically and saved to the configuration file. No matter how the password was entered, it appears in the configuration file with the keyword encrypted and the encrypted value.

If the administrator wants to manually copy a password that was configured on one switch (for instance, switch B) to another switch (for instance, switch A), the administrator must add encrypted in front of this encrypted password when entering the enable command in switch A. In this way, the two switches will have the same password.

Passwords are encrypted by default. You only are required to use the encrypted keyword when you are actually entering an encrypted keyword.

Examples

Example 1 - The command sets a password that has already been encrypted. It will copied to the configuration file just as it is entered. To use it, the user must know its unencrypted form.

```
switchxxxxxx(config)# enable password encrypted
4b529f21c93d4706090285b0c10172eb073ffebc4
```

Example 2 - The command sets an unencrypted password for level 7 (it will be encrypted in the configuration file).

```
switchxxxxxx(config)# enable password level 7 let-me-in
```

3.9. service password-recovery

Use the `service password-recovery` Global Configuration mode command to enable the password-recovery mechanism. This mechanism allows an end user, with physical access to the console port of the device, to enter the boot menu and trigger the password recovery process. Use the no service password-recovery command to disable the password-recovery mechanism. When the password-recovery mechanism is disabled, accessing the boot menu is still allowed and the user can trigger the password recovery process. The difference is, that in this case, all the configuration files and all the user files are removed. The following log message is generated to the terminal: "All the configuration and user files were removed".

Syntax

- service password-recovery
- no service password-recovery

Parameters

N/A

Default Configuration

The service password recovery is enabled by default.

Command Mode

Global Configuration mode

User Guidelines

- If password recovery is enabled, the user can access the boot menu and trigger the password recovery in the boot menu. All configuration files and user files are kept.
- If password recovery is disabled, the user can access the boot menu and trigger the password recovery in the boot menu. The configuration files and user files are removed.
- If a device is configured to protect its sensitive data with a user-defined passphrase for (Secure Sensitive Data), then the user cannot trigger the password recovery from the boot menu even if password recovery is enabled.
- If a device is configured to protect its sensitive data with a user-defined passphrase for (Secure Sensitive Data), then the user cannot trigger the password recovery from the boot menu even if password recovery is enabled.

Example

The following command disables password recovery:

```
switchxxxxxx(config)# no service password recovery
Note that choosing to use Password recovery option in the Boot Menu during the
boot process will remove the configuration files and the user files.
Would you like to continue ? Y/N.
```

3.10. username

Use the `username` Global Configuration mode command to establish a username-based authentication system. Use the no form to remove a user name.

Syntax

- username name {nopassword | {password {unencrypted-password | {encrypted encrypted-password}}} | {privilege privilege-level {unencrypted-password | {encrypted encrypted-password}}}
- no username name

Parameters

- name - The name of the user. (Range: 1–20 characters)
- nopassword - No password is required for this user to log in.
- password - Specifies the password for this username. (Range: 1–64)
- unencrypted-password - The authentication password for the user. (Range: 1–159)
- encrypted encrypted-password - Specifies that the password is MD5 encrypted. Use this keyword to enter a password that is already encrypted (for instance that you copied from another the configuration file of another device). (Range: 1–40)
- privilege privilege-level - Privilege level for which the password applies. If not specified the level is 1. (Range: 1–15).

Default Configuration

No user is defined.

Command Mode

Global Configuration mode

Usage Guidelines

The last level 15 user (regardless of whether it is the default user or any user) cannot be removed and cannot be a remote user.

Examples

Example 1 - Sets an unencrypted password for user tom (level 15). It will be encrypted in the configuration file.

```
switchxxxxxx(config)# username tom password 1234
```

Example 2 - Sets a password for user jerry (level 15) that has already been encrypted. It will be copied to the configuration file just as it is entered. To use it, the user must know its unencrypted form.

```
switchxxxxxx(config)# username jerry privilege 15 encrypted
4b529f21c93d4706090285b0c10172eb073ffebc4
```

3.11. show users accounts

The `show users accounts` Privileged EXEC mode command displays information about the users local database.

Syntax

- show users accounts

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

By default a Level 15 user with username “admin” and password “admin” exists.

Example

The following example displays information about the users local database:

```
switchxxxxxx# show users accounts
Password
Username Privilege Expiry date
-------- --------- -----------
Bob 15 Jan 18 2005
Robert 15 Jan 19 2005
Smith 15
```

The following table describes the significant fields shown in the display:

Field	Description
Username	The user name.
Privilege	The user’s privilege level.
Password Expiry date	The user's password expiration date.

3.12. aaa accounting login

Use the `aaa accounting login` command in Global Configuration mode to enable accounting of device management sessions. Use the no form of this command to disable accounting.

Syntax

- aaa accounting login start-stop group {radius | tacacs+}
- no aaa accounting login start-stop

Parameters

- group radius - Uses a RADIUS server for accounting.
- group tacacs+ - Uses a TACACS+ server for accounting.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

This command enables the recording of up to 128 device management sessions (Telnet, serial and WEB but not SNMP).

It records only users that were identified with a username (e.g. a user that was logged in with a line password is not recorded).

If accounting is activated, the device sends a “start”/“stop” messages to a RADIUS server when a user logs in / logs out respectively.

The device uses the configured priorities of the available RADIUS/TACACS+ servers in order to select the RADIUS/TACACS+ server.

The following table describes the supported RADIUS accounting attributes values, and in which messages they are sent by the switch.

Name	Start Message	Stop Message	Description
User-Name (1)	Yes	Yes	User’s identity.
NAS-IP-Address (4)	Yes	Yes	The switch IP address that is used for the session with the RADIUS server.

Class (25)	Yes	Yes	Arbitrary value is included in all accounting packets for a specific session.
Called-Station-ID (30)	Yes	Yes	The switch IP address that is used for the management session.
Calling-Station-ID (31)	Yes	Yes	The user IP address.
Acct-Session-ID (44)	Yes	Yes	A unique accounting identifier.
Acct-Authentic (45)	Yes	Yes	Indicates how the supplicant was authenticated.
Acct-Session-Time (46)	No	Yes	Indicates how long the user was logged in.
Acct-Terminate-Cau se (49)	No	Yes	Reports why the session was terminated.

The following table describes the supported TACACS+ accounting arguments and in which messages they are sent by the switch.

Name	Description	Start Message	Stop Message
task_id	A unique accounting session identifier.	Yes	Yes
user	username that is entered for login authentication	Yes	Yes
rem-addr	IP address.of the user	Yes	Yes
elapsed-time	Indicates how long the user was logged in.	No	Yes
reason	Reports why the session was terminated.	No	Yes

Example

```
switchxxxxxx(config)# aaa accounting login start-stop group radius
```

3.13. aaa accounting dot1x

To enable accounting of 802.1x sessions, use the `aaa accounting dot1x` Global Configuration mode command. Use the no form of this command to disable accounting.

Syntax

- aaa accounting dot1x start-stop group radius
- no aaa accounting dot1x start-stop group radius

Parameters

N/A

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

This command enables the recording of 802.1x sessions.

If accounting is activated, the device sends start/stop messages to a RADIUS server when a user logs in / logs out to the network, respectively.

The device uses the configured priorities of the available RADIUS servers in order to select the RADIUS server.

If a new supplicant replaces an old supplicant (even if the port state remains authorized), the software sends a stop message for the old supplicant and a start message for the new supplicant.

In multiple sessions mode (dot1x multiple-hosts authentication), the software sends start/stop messages for each authenticated supplicant.

In multiple hosts mode (dot1x multiple-hosts), the software sends start/stop messages only for the supplicant that has been authenticated.

The software does not send start/stop messages if the port is force-authorized.

The software does not send start/stop messages for hosts that are sending traffic on the guest VLAN or on the unauthenticated VLANs.

The following table describes the supported Radius accounting Attributes Values and when they are sent by the switch.

Name	Start	Stop	Description
User-Name (1)	Yes	Yes	Supplicant's identity.
NAS-IP-Address (4)	Yes	Yes	The switch IP address that is used for the session with the RADIUS server.
NAS-Port (5)	Yes	Yes	The switch port from where the supplicant has logged in.
Class (25)	Yes	Yes	The arbitrary value that is included in all accounting packets for a specific session.
Called-Station-ID (30)	Yes	Yes	The switch MAC address.

Calling-Station-ID (31)	Yes	Yes	The supplicant MAC address.
Acct-Session-ID (44)	Yes	Yes	A unique accounting identifier.
Name	Start	Stop	Description
Acct-Authentic (45)	Yes	Yes	Indicates how the supplicant was authenticated.
Acct-Session-Time (46)	No	Yes	Indicates how long the supplicant was logged in.
Acct-Terminate-Cause (49)	No	Yes	Reports why the session was terminated.
Nas-Port-Type (61)	Yes	Yes	Indicates the supplicant physical port type.

Example

```
switchxxxxxx(config)# aaa accounting dot1x start-stop group radius
```

3.14. show accounting

The `show accounting` EXEC mode command displays information as to which type of accounting is enabled on the switch.

Syntax

- show accounting

Parameters

N/A

Default Configuration

N/A

Command Mode

User EXEC mode

Example

The following example displays information about the accounting status.

```
switchxxxxxx# show accounting
Login: Radius
802.1x: Disabled
```

3.15. passwords complexity enable

Use the `passwords complexity enable` Global Configuration mode command to enforce minimum password complexity. The no form of this command disables enforcing password complexity.

Syntax

- passwords complexity enable
- no passwords complexity enable

Parameters

N/A

Default Configuration

Enabled

Command Mode

Global Configuration mode

User Guidelines

If password complexity is enabled, the user is forced to enter a password that:

- Has a minimum length of 8 characters.
- Contains characters from at least 3 character classes (uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard).
- Is different from the current password.
- Contains no character that is repeated more than 3 times consecutively.
- Does not repeat or reverse the user name or any variant reached by changing the case of the characters.
- Does not repeat or reverse the manufacturer's name or any variant reached by changing the case of the characters.

You can control the above attributes of password complexity with specific commands described in this section.

If you have previously configured other complexity settings, then those settings are used. This command does not wipe out the other settings. It works only as a toggle.

Example

The following example configures requiring complex passwords that fulfill the minimum requirements specified in the User Guidelines above.

```
switchxxxxxx(config)# passwords complexity enable
switchxxxxxx# show passwords configuration
Passwords aging is enabled with aging time 180 days.
Passwords complexity is enabled with the following attributes:
Minimal length: 3 characters
Minimal classes: 3
New password must be different than the current: Enabled
Maximum consecutive same characters: 3
New password must be different than the user name: Enabled New password must be
different than the manufacturer name: Enabled
switchxxxxxx#
```

3.16. passwords complexity

Use the `passwords complexity` Global Configuration mode commands to control the minimum requirements from a password when password complexity is enabled. Use the no form of these commands to return to default.

Syntax

- passwords complexity {min-length number} | {min-classes number} | not-current | {no-repeat number} | not-username | not-manufacturer-name
- no passwords complexity min-length | min-classes | not-current | no-repeat | not-username | not-manufacturer-name

Parameters

- min-length number - Sets the minimal length of the password. (Range: 0– 64)
- min-classes number - Sets the minimal character classes (uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard). (Range: 0–4)
- not-current - Specifies that the new password cannot be the same as the current password.
- no-repeat number - Specifies the maximum number of characters in the new password that can be repeated consecutively. Zero specifies that there is no limit on repeated characters. (Range: 0–16)
- not-username - Specifies that the password cannot repeat or reverse the user name or any variant reached by changing the case of the characters.
- not-manufacturer-name - Specifies that the password cannot repeat or reverse the manufacturer's name or any variant reached by changing the case of the characters.

Default Configuration

The minimal length is 8.

The number of classes is 3.

The default for no-repeat is 3.

All the other controls are enabled by default.

Command Mode

Global Configuration mode

Example

The following example configures the minimal required password length to 8 characters.

```
switchxxxxxx(config)# passwords complexity min-length 8
```

3.17. passwords aging

Use the `passwords aging` Global Configuration mode command to enforce password aging. Use the no form of this command to return to default.

Syntax

- passwords aging days
- no passwords aging

Parameters

- days - Specifies the number of days before a password change is forced. You can use 0 to disable aging. (Range: 0–365).

Default Configuration

180

Command Mode

Global Configuration mode

User Guidelines

Aging is relevant only to users of the local database with privilege level 15 and to enable a password of privilege level 15.

To disable password aging, use passwords aging 0.

Using no passwords aging sets the aging time to the default.

Example

The following example configures the aging time to be 24 days.

```
switchxxxxxx(config)# passwords aging 24
```

3.18. show passwords configuration

The `show passwords configuration` Privileged EXEC mode command displays information about the password management configuration.

Syntax

- show passwords configuration

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show passwords configuration
Passwords aging is enabled with aging time 180 days.
Passwords complexity is enabled with the following attributes:
 Minimal length: 3 characters
 Minimal classes: 3
 New password must be different than the current: Enabled
 Maximum consecutive same characters: 3
 New password must be different than the user name: Enabled
 New password must be different than the manufacturer name: Enabled
Enable Passwords
Level Line Passwords
 Line
----- --------------
1 Console
15 Telnet
 SSH
```

4. ACL Commands

4.1. ip access-list (IP extended)

Use the `ip access-list` extended Global Configuration mode command to name an IPv4 access list (ACL) and to place the device in IPv4 Access List Configuration mode. All commands after this command refer to this ACL. The rules (ACEs) for this ACL are defined in the `permit (IP)` and `deny (IP)` commands. The `service-acl input` command is used to attach this ACL to an interface.

Use the no form of this command to remove the access list.

Syntax

- ip access-list extended acl-name
- no ip access-list extended acl-name

Parameters

- acl-name - Name of the IPv4 access list. (Range 1-32 characters)

Default Configuration

No IPv4 access list is defined.

Command Mode

Global Configuration mode

User Guidelines

An IPv4 ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or policy maps cannot have the same name.

Example

```
switchxxxxxx(config)# ip access-list extended server
switchxxxxxx(config-ip-al)#
```

4.2. permit (IP)

Use the `permit IP` Access-list Configuration mode command to set permit conditions for an IPv4 access list (ACL). Permit conditions are also known as access control entries (ACEs). Use the no form of the command to remove the access control entry.

Syntax

- permit protocol {any | source source-wildcard} {any | destination destination-wildcard} [ace-priority priority] [dscp number | precedence number] [time-range time-range-name] [log-input]
- permit icmp {any | source source-wildcard} {any | destination destination-wildcard} [any | icmp-type] [any | icmp-code]] [ace-priority priority] [dscp number | precedence number] [time-range time-range-name] [log-input]
- permit igmp {any | source source-wildcard} {any | destination destination-wildcard}[igmp-type] [ace-priority priority] [dscp number | precedence number] [time-range time-range-name] [log-input]
- permit tcp {any | source source-wildcard} {any|source-port/port-range}{any | destination destination-wildcard} {any|destination-port/port-range} [ace-priority priority] [dscp number | precedence number] [match-all list-of-flags] [time-range time-range-name] [log-input]

- permit udp {any | source source-wildcard} {any|source-port/port-range} {any | destination destination-wildcard} {any|destination-port/port-range} [ace-priority priority] [dscp number | precedence number] [time-range time-range-name] [log-input]
- no permit protocol {any | source source-wildcard} {any | destination destination-wildcard} [dscp number | precedence number][time-range time-range-name] [log-input]
- no permit icmp {any | source source-wildcard} {any | destination destination-wildcard} [any | icmp-type] [any | icmp-code]] [dscp number | precedence number][time-range time-range-name] [log-input]
- no permit igmp {any | source source-wildcard} {any | destination destination-wildcard}[igmp-type] [dscp number | precedence number] [time-range time-range-name] [log-input]
- no permit tcp {any | source source-wildcard} {any|source-port/port-range}{any | destination destination-wildcard} {any|destination-port/port-range} [dscp number | precedence number] [match-all list-of-flags] [time-range time-range-name] [log-input]
- no permit udp {any | source source-wildcard} {any|source-port/port-range} {any | destination destination-wildcard} {any|destination-port/port-range} [dscp number | precedence number] [time-range time-range-name] [log-input]

Parameters

- protocol - The name or the number of an IP protocol. Available protocol names are: icmp, igmp, ip, tcp, egp, igp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis. To match any protocol, use the ip keyword.(Range: 0–255)
- source - Source IP address of the packet.
- source-wildcard - Wildcard bits to be applied to the source IP address. Use ones in the bit position that you want to be ignored.
- destination - Destination IP address of the packet.
- destination-wildcard - Wildcard bits to be applied to the destination IP address. Use ones in the bit position that you want to be ignored.
- priority - Specify the priority of the access control entry (ACE) in the access control list (ACL). "1" value represents the highest priority and "2147483647" number represents the lowest priority.(Range: 1-2147483647)
- dscp number - Specifies the DSCP value.
- precedence number - Specifies the IP precedence value.
- icmp-type - Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain-name-request, domain-name-reply, skip, photuris. (Range: 0–255)
- icmp-code - Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- igmp-type - IGMP packets can be filtered by IGMP message type. Enter a number or one of the following values: host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3. (Range: 0–255)
- destination-port - Specifies the UDP/TCP destination port. You can enter range of ports by using hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values:

bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177).(Range: 0–65535).

- source-port - Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)
- match-all list-of-flags - List of TCP flags that should occur. If a flag should be set, it is prefixed by “+”. If a flag should be unset, it is prefixed by “-”. Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
- time-range-name - Name of the time range that applies to this permit statement. (Range: 1–32)
- log-input - Specifies sending an informational SYSLOG message about the packet that matches the entry. Because forwarding/dropping is done in hardware and logging is done in software, if a large number of packets match an ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

Default Configuration

No IPv4 access list is defined.

Command Mode

IP Access-list Configuration mode

User Guidelines

If a range of ports is used for source port in an ACE, it is not counted again, if it is also used for a source port in another ACE. If a range of ports is used for the destination port in an ACE, it is not counted again if it is also used for destination port in another ACE.

If a range of ports is used for source port it is counted again if it is also used for destination port.

If ace-priority is omitted, the system sets the rule's priority to the current highest priority ACE (in the current ACL) + 20. The ACE-priority must be unique per ACL.If the user types already existed priority, then the command is rejected.

Example

```
switchxxxxxx(config)# ip access-list extended server
switchxxxxxx(config-ip-al)# permit ip 176.212.0.0 00.255.255 any
```

4.3. deny (IP)

Use the `deny IP` Access-list Configuration mode command to set deny conditions for IPv4 access list. Deny conditions are also known as access control entries (ACEs). Use the no form of the command to remove the access control entry.

Syntax

- deny protocol {any | source source-wildcard} {any | destination destination-wildcard} [ace-priority priority] [dscp number | precedence number] [time-range time-range-name] [disable-port |log-input]
- deny icmp {any | source source-wildcard} {any | destination destination-wildcard} [any | icmp-type] [any | icmp-code]][ace-priority priority] [dscp number | precedence number] [time-range time-range-name] [disable-port |log-input] deny igmp {any | source source-wildcard} {any | destination destination-wildcard}[igmp-type][ace-priority priority] [dscp number | precedence number] [time-range time-range-name] [disable-port |log-input]
- deny tcp {any | source source-wildcard} {any|source-port/port-range}{any | destination destination-wildcard} {any|destination-port/port-range} [ace-priority priority] [dscp number | precedence number] [match-all list-of-flags][time-range time-range-name] [disable-port |log-input]
- deny udp {any | source source-wildcard} {any|source-port/port-range} {any | destination destination-wildcard} {any|destination-port/port-range} [ace-priority priority] [dscp number | precedence number] [time-range time-range-name] [disable-port |log-input]
- no deny protocol {any | source source-wildcard} {any | destination destination-wildcard} [dscp number | precedence number] [time-range time-range-name] [disable-port |log-input]
- no deny icmp {any | source source-wildcard} {any | destination destination-wildcard} [any | icmp-type] [any | icmp-code]] [dscp number | precedence number][time-range time-range-name] [disable-port |log-input]
- no deny igmp {any | source source-wildcard} {any | destination destination-wildcard}[igmp-type] [dscp number | precedence number] [time-range time-range-name] [disable-port |log-input]
- no deny tcp {any | source source-wildcard} {any|source-port/port-range}{any | destination destination-wildcard} {any|destination-port/port-range} [dscp number | precedence number] [match-all list-of-flags] [time-range time-range-name] [disable-port |log-input]
- no deny udp {any | source source-wildcard} {any|source-port/port-range} {any | destination destination-wildcard} {any|destination-port/port-range} [dscp number | precedence number] [time-range time-range-name] [disable-port |log-input]

Parameters

- protocol - The name or the number of an IP protocol. Available protocol names: icmp, igmp, ip, tcp, egp, igp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis. To match any protocol, use the Ip keyword. (Range: 0–255)
- source - Source IP address of the packet.
- source-wildcard - Wildcard bits to be applied to the source IP address. Use 1s in the bit position that you want to be ignored.
- destination - Destination IP address of the packet.
- destination-wildcard - Wildcard bits to be applied to the destination IP address. Use 1s in the bit position that you want to be ignored.
- priority - Specify the priority of the access control entry (ACE) in the access control list (ACL). "1" value represents the highest priority and "2147483647" number represents the lowest priority.(Range: 1-2147483647)
- dscp number - Specifies the DSCP value.
- precedence number - Specifies the IP precedence value.

- icmp-type - Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain-name-request, domain-name-reply, skip, photuris. (Range: 0–255)
- icmp-code - Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- igmp-type - IGMP packets can be filtered by IGMP message type. Enter a number or one of the following values: host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3. (Range: 0–255)
- destination-port - Specifies the UDP/TCP destination port. You can enter range of ports by using hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), non500-isakmp (4500), ntp (123), rip (520), snmp 161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). (Range: 0–65535)
- source-port - Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)
- match-all list-of-flags - List of TCP flags that should occur. If a flag should be set it is prefixed by “+”.If a flag should be unset it is prefixed by “-”. Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
- time-range-name - Name of the time range that applies to this permit statement. (Range: 1–32)
- disable-port - The Ethernet interface is disabled if the condition is matched.
- log-input - Specifies sending an informational syslog message about the packet that matches the entry. Because forwarding/dropping is done in hardware and logging is done in software, if a large number of packets match an ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

Default Configuration

No IPv4 access list is defined.

Command Mode

IP Access-list Configuration mode

User Guidelines

The number of TCP/UDP ranges that can be defined in ACLs is limited. If a range of ports is used for a source port in ACE it is not counted again if it is also used for source port in another ACE. If a range of ports is used for destination port in ACE it is not counted again if it is also used for destination port in another ACE.

If a range of ports is used for source port, it is counted again if it is also used for destination port.

If ace-priority is omitted, the system sets the rule's priority to the current highest priority ACE (in the current ACL) + 20. The ACE-priority must be unique per ACL.If the user types already existed priority, then the command is rejected.

Example

```
switchxxxxxx(config)# ip access-list extended server
switchxxxxxx(config-ip-al)# deny ip 176.212.0.0 00.255.255 any
```

4.4. ipv6 access-list (IPv6 extended)

Use the `ipv6 access-list` Global Configuration mode command to define an IPv6 access list (ACL) and to place the device in Ipv6 Access-list Configuration mode. All commands after this command refer to this ACL. The rules (ACEs) for this ACL are defined in the `permit (IPv6)` and `deny (IPv6)` commands. The `service-acl input` command is used to attach this ACL to an interface.

Use the no form of this command to remove the access list.

Syntax

- ipv6 access-list [acl-name]
- no ipv6 access-list [acl-name]

Parameters

- acl-name - Name of the IPv6 access list. Range 1-32 characters.

Default Configuration

No IPv6 access list is defined.

Command Mode

Global Configuration mode

User Guidelines

IPv6 ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or policy maps cannot have the same name.

Every IPv6 ACL has an implicit permit icmp any any nd-ns any, permit icmp any any nd-na any, and deny ipv6 any any statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.)

The IPv6 neighbor discovery process uses the IPv6 network layer service, therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, uses a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Example

```
switchxxxxxx(config)# ipv6 access-list acl1
switchxxxxxx(config-ip-al)# permit tcp 2001:0DB8:0300:0201::/64 any any 80
```

4.5. permit (IPv6)

Use `the permit` command in Ipv6 Access-list Configuration mode to set permit conditions (ACEs) for IPv6 ACLs. Use the no form of the command to remove the access control entry.

Syntax

- permit protocol {any |{source-prefix/length}{any | destination-prefix/length} [ace-priority priority][dscp number | precedence number] [time-range time-range-name] [log-input]
- permit icmp {any | {source-prefix/length}{any | destination-prefix/length} {any|icmp-type} {any|icmp-code} [ace-priority priority][dscp number | precedence number] [time-range time-range-name] [log-input]
- permit tcp {any | {source-prefix/length} {any | source-port | source-port-range}}{any | destination-prefix/length} {any | destination-port | destination-port-range} [ace-priority priority][dscp number | precedence number] [match-all list-of-flags] [time-range time-range-name] [log-input]
- permit udp {any | {source-prefix/length}} {any | source-port | source-port-range}}{any | destination-prefix/length} {any | destination-port | destination-port-range} [ace-priority priority][dscp number | precedence number][time-range time-range-name] [log-input]
- no permit protocol {any |{source-prefix/length}{any | destination-prefix/length} [dscp number | precedence number] [time-range time-range-name] [log-input]
- no permit icmp {any | {source-prefix/length}{any | destination-prefix/length} {any|icmp-type} {any|icmp-code} [dscp number | precedence number] [time-range time-range-name] [log-input]
- no permit tcp {any | {source-prefix/length} {any | source-port | source-port-range}}{any | destination- prefix/length} {any| destination-port | destination-port-range} [dscp number | precedence number] [match-all list-of-flags] [time-range time-range-name] [log-input]
- no permit udp {any | {source-prefix/length}} {any | source-port | source-port-range}}{any | destination-prefix/length} {any| destination-port | destination-port-range} [dscp number | precedence number] [time-range time-range-name] [log-input]

Parameters

- protocol - The name or the number of an IP protocol. Available protocol names are: icmp (58), tcp (6) and udp (17). To match any protocol, use the ipv6 keyword. (Range: 0–255)
- source-prefix/length - The source IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.
- destination-prefix/length - The destination IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.
- priority - Specify the priority of the access control entry (ACE) in the access control list (ACL). "1" value represents the highest priority and "2147483647" number represents the lowest priority.(Range: 1-2147483647)
- dscp number - Specifies the DSCP value. (Range: 0–63)
- precedence number - Specifies the IP precedence value.
- icmp-type - Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: destination-unreachable (1), packet-too-big (2), time-exceeded (3), parameter-problem (4), echo-request (128), echo-reply

(129), mld-query (130), mld-report (131), mldv2-report (143), mld-done (132), router-solicitation (133), router-advertisement (134), nd-ns (135), nd-na (136). (Range: 0–255)

- icmp-code - Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- destination-port - Specifies the UDP/TCP destination port. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), non500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). (Range: 0–65535)
- destination-port-range - Specifies the UDP/TCP destination port range. You can enter a range of ports by using a hyphen. E.g. 20 - 21.
- source-port - Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)
- source-port-range - Specifies the UDP/TCP source port range. You can enter a range of ports by using a hyphen. E.g. 20 - 21.
- match-all list-of-flag - List of TCP flags that should occur. If a flag should be set it is prefixed by “+”.If a flag should be unset it is prefixed by “-”. Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
- time-range-name - Name of the time range that applies to this permit statement. (Range: 1–32)
- log-input - Specifies sending an informational SYSLOG message about the packet that matches the entry. Because forwarding/dropping is done in hardware and logging is done in software, if a large number of packets match an ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

Default Configuration

No IPv6 access list is defined.

Command Mode

Ipv6 Access-list Configuration mode

User Guidelines

If a range of ports is used for the destination port in an ACE, it is not counted again if it is also used for destination port in another ACE.

The number of TCP/UDP ranges that can be defined in ACLs is limited. If a range of ports is used for a source port in ACE, it is not counted again if it is also used for a source port in another ACE. If a range of ports is used for destination port in ACE it is not counted again if it is also used for destination port in another ACE.

If a range of ports is used for source port it is counted again if it is also used for destination port.

If ace-priority is omitted, the system sets the rule's priority to the current highest priority ACE (in the current ACL) + 20. The ACE-priority must be unique per ACL.If the user types already existed priority, then the command is rejected.

Example

This example defines an ACL by the name of server and enters a rule (ACE) for tcp packets.

```
switchxxxxxx(config)# ipv6 access-list server
switchxxxxxx(config-ipv6-al)# permit tcp 3001::2/64 any any 80
```

4.6. deny (IPv6)

Use the `deny` command in Ipv6 Access-list Configuration mode to set permit conditions (ACEs) for IPv6 ACLs. Use the no form of the command to remove the access control entry.

Syntax

- deny protocol {any | {source-prefix/length}{any | destination-prefix/length} [ace-priority priority][dscp number | precedence number] [time-range time-range-name] [disable-port |log-input]
- deny icmp {any | {source-prefix/length}{any | destination-prefix/length} {any|icmp-type} {any|icmp-code} [ace-priority priority][dscp number | precedence number] [time-range time-range-name] [disable-port |log-input]
- deny tcp {any | {source-prefix/length} {any | source-port | source-port-range}}{any | destination-prefix/length} {any| destination-port | destination-port-range} [ace-priority priority][dscp number | precedence number] [match-all list-of-flags] [time-range time-range-name] [disable-port |log-input]
- deny udp {any | {source-prefix/length}} {any | source-port | source-port-range}}{any | destination-prefix/length} {any| destination-port | destination-port-range} [ace-priority priority][dscp number | precedence number] [time-range time-range-name] [disable-port |log-input]
- no deny protocol {any | {source-prefix/length}{any | destination-prefix/length} [dscp number | precedence number] [time-range time-range-name] [disable-port |log-input]
- no deny icmp {any | {source-prefix/length}{any | destination-prefix/length} {any|icmp-type} {any|icmp-code} [dscp number | precedence number] [time-range time-range-name] [disable-port |log-input]
- no deny tcp {any | {source-prefix/length} {any | source-port | source-port-range}}{any | destination-prefix/length} {any| destination-port | destination-port-range} [dscp number | precedence number] [match-all list-of-flags] [time-range time-range-name] [disable-port |log-input]
- no deny udp {any | {source-prefix/length}} {any | source-port | source-port-range}}{any | destination-prefix/length} {any| destination-port | destination-port-range} [dscp number | precedence number] [time-range time-range-name] [disable-port |log-input]

Parameters

- protocol - The name or the number of an IP protocol. Available protocol names are: icmp (58), tcp (6) and udp (17). To match any protocol, use the ipv6 keyword. (Range: 0–255)
- source-prefix/length - The source IPv6 network or class of networks about which to set permit conditions. This argument must be in the format documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.

- destination-prefix/length - The destination IPv6 network or class of networks about which to set permit conditions. This argument must be in the format documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.
- priority - Specify the priority of the access control entry (ACE) in the access control list (ACL). "1" value represents the highest priority and "2147483647" number represents the lowest priority.(Range: 1-2147483647)
- dscp number - Specifies the DSCP value. (Range: 0–63)
- precedence number - Specifies the IP precedence value.
- icmp-type - Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: destination-unreachable (1), packet-too-big (2), time-exceeded (3), parameter-problem (4), echo-request (128), echo-reply (129), mld-query (130), mld-report (131), mldv2-report (143), mld-done (132), router-solicitation (133), router-advertisement (134), nd-ns (135), nd-na (136). (Range: 0–255)
- icmp-code - Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- destination-port - Specifies the UDP/TCP destination port. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data 20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), non500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). (Range: 0–65535)
- destination-port-range - Specifies the UDP/TCP destination port range. You can enter a range of ports by using a hyphen. E.g. 20 - 21.
- source-port - Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)
- source-port-range - Specifies the UDP/TCP source port range. You can enter a range of ports by using a hyphen. E.g. 20 - 21.
- match-all list-of-flags - List of TCP flags that should occur. If a flag should be set it is prefixed by “+”.If a flag should be unset it is prefixed by “-”. Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
- time-range-name - Name of the time range that applies to this permit statement. (Range: 1–32)
- disable-port - The Ethernet interface is disabled if the condition is matched.
- log-input - Specifies sending an informational syslog message about the packet that matches the entry. Because forwarding/dropping is done in hardware and logging is done in software, if a large number of packets match an ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

Default Configuration

No IPv6 access list is defined.

Command Mode

Ipv6 Access-list Configuration mode

User Guidelines

The number of TCP/UDP ranges that can be defined in ACLs is limited. If a range of ports is used for source port in ACE it is not counted again if it is also used for source port in another ACE. If a range of ports is used for a destination port in ACE it is not counted again if it is also used for a destination port in another ACE.

If a range of ports is used for source port it is counted again if it is also used for destination port.

If ace-priority is omitted, the system sets the rule's priority to the current highest priority ACE (in the current ACL) + 20. The ACE-priority must be unique per ACL.If the user types already existed priority, then the command is rejected.

Example

```
switchxxxxxx(config)# ipv6 access-list server
switchxxxxxx(config-ipv6-al)# deny tcp 3001::2/64 any any 80
```

4.7. mac access-list

Use the `mac access-list` Global Configuration mode command to define a Layer 2 access list (ACL) based on source MAC address filtering and to place the device in MAC Access-list Configuration mode. All commands after this command refer to this ACL. The rules (ACEs) for this ACL are defined in the `permit (MAC)` and `deny (MAC)` commands. The `service-acl input` command is used to attach this ACL to an interface.

Use the no form of this command to remove the access list.

Syntax

- mac access-list extended acl-name
- no mac access-list extended acl-name

Parameters

- acl-name - Specifies the name of the MAC ACL (Range: 1–32 characters).

Default Configuration

No MAC access list is defined.

Command Mode

Global Configuration mode

User Guidelines

A MAC ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or policy maps cannot have the same name

If ace-priority is omitted, the system sets the rule's priority to the current highest priority ACE (in the current ACL) + 20. The ACE-priority must be unique per ACL.If the user types already existed priority, then the command is rejected.

Example

```
switchxxxxxx(config)# mac access-list extended server1
switchxxxxxx(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
```

4.8. permit (MAC)

Use the `permit` command in MAC Access-list Configuration mode to set permit conditions (ACEs) for a MAC ACL. Use the no form of the command to remove the access control entry.

Syntax

- permit {any | source source-wildcard} {any | destination destination-wildcard} [ace-priority priority][eth-type 0 | aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000] [vlan vlan-id] [cos cos cos-wildcard] [time-range time-range-name] [log-input]
- no permit {any | source source-wildcard} {any | destination destination-wildcard} [eth-type 0 | aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000] [vlan vlan-id] [cos cos cos-wildcard] [time-range time-range-name] [log-input]

Parameters

- source - Source MAC address of the packet.
- source-wildcard - Wildcard bits to be applied to the source MAC address. Use 1s in the bit position that you want to be ignored.
- destination - Destination MAC address of the packet.
- destination-wildcard - Wildcard bits to be applied to the destination MAC address. Use 1s in the bit position that you want to be ignored.
- priority - Specify the priority of the access control entry (ACE) in the access control list (ACL). "1" value represents the highest priority and "2147483647" number represents the lowest priority.(Range: 1-2147483647)
- eth-type - The Ethernet type in hexadecimal format of the packet.
- vlan-id - The VLAN ID of the packet. (Range: 1–4094)
- cos - The Class of Service of the packet. (Range: 0–7)
- cos-wildcard - Wildcard bits to be applied to the CoS.
- time-range-name - Name of the time range that applies to this permit statement. (Range: 1–32)
- log-input - Specifies sending an informational SYSLOG message about the packet that matches the entry. Because forwarding/dropping is done in hardware and logging is done in software, if a large number of packets match an ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

User Guidelines

A MAC ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or policy maps cannot have the same name

If ace-priority is omitted, the system sets the rule's priority to the current highest priority ACE (in the current ACL) + 20. The ACE-priority must be unique per ACL.If the user types already existed priority, then the command is rejected.

Default Configuration

No MAC access list is defined.

Command Mode

MAC Access-list Configuration mode

Example

```
switchxxxxxx(config)# mac access-list extended server1
switchxxxxxx(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
```

4.9. deny (MAC)

Use the `deny` command in MAC Access-list Configuration mode to set deny conditions (ACEs) for a MAC ACL. Use the no form of the command to remove the access control entry.

Syntax

- deny {any | source source-wildcard} {any | destination destination-wildcard} [ace-priority priority][{eth-type 0}| aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000] [vlan vlan-id] [cos cos cos-wildcard] [time-range time-range-name] [disable-port |log-input]
- no deny {any | source source-wildcard} {any | destination destination-wildcard} [{eth-type 0}| aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000] [vlan vlan-id] [cos cos cos-wildcard] [time-range time-range-name] [disable-port |log-input]

Parameters

- source - Source MAC address of the packet.
- source-wildcard - Wildcard bits to be applied to the source MAC address. Use ones in the bit position that you want to be ignored.
- destination - Destination MAC address of the packet.
- destination-wildcard - Wildcard bits to be applied to the destination MAC address. Use 1s in the bit position that you want to be ignored.
- priority - Specify the priority of the access control entry (ACE) in the access control list (ACL). "1" value represents the highest priority and "2147483647" number represents the lowest priority.(Range: 1-2147483647) eth-type - The Ethernet type in hexadecimal format of the packet.
- vlan-id - The VLAN ID of the packet. (Range: 1–4094).
- cos - The Class of Service of the packet.(Range: 0–7).
- cos-wildcard - Wildcard bits to be applied to the CoS.
- time-range-name - Name of the time range that applies to this permit statement. (Range: 1–32)
- disable-port - The Ethernet interface is disabled if the condition is matched.
- log-input - Specifies sending an informational syslog message about the packet that matches the entry. Because forwarding/dropping is done in hardware and logging is done in software, if a large number of packets match an ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

Default Configuration

No MAC access list is defined.

Command Mode

MAC Access-list Configuration mode

User Guidelines

A MAC ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or policy maps cannot have the same name

If ace-priority is omitted, the system sets the rule's priority to the current highest priority ACE (in the current ACL) + 20. The ACE-priority must be unique per ACL.If the user types already existed priority, then the command is rejected.

Example

```
switchxxxxxx(config)# mac access-list extended server1
switchxxxxxx(config-mac-al)# deny 00:00:00:00:00:01 00:00:00:00:00:ff any
```

4.10. service-acl input

Use the `service-acl input` command in Interface Configuration mode to bind an access list(s) (ACL) to an interface.

Use the no form of this command to remove all ACLs from the interface.

Syntax

- sevice-acl input acl-name1 [acl-name2] [default-action {deny-any | permit-any}]
- no service-acl input

Parameters

- acl-name - Specifies an ACL to apply to the interface. See the user guidelines. (Range: 1–32 characters).
- deny-any - Deny all packets (that were ingress at the port) that do not meet the rules in this ACL.
- permit-any - Forward all packets (that were ingress at the port) that do not meet the rules in this ACL.

Default Configuration

No ACL is assigned.

Command Mode

Interface Configuration mode (Ethernet, Port-Channel,,VLAN)

User Guidelines

The following rules govern when ACLs can be bound or unbound from an interface:

- IPv4 ACLs and IPv6 ACLs can be bound together to an interface.
- A MAC ACL cannot be bound on an interface which already has an IPv4 ACL or IPv6 ACL bound to it.
- Two ACLs of the same type cannot be bound to a port.
- An ACL cannot be bound to a port that is already bound to an ACL, without first removing the current ACL. Both ACLs must be mentioned at the same time in this command.
- MAC ACLs that include a VLAN as match criteria cannot be bound to a VLAN. ACLs with time-based configuration on one of its ACEs cannot be bound to a VLAN.
- ACLs with the action Shutdown cannot be bound to a VLAN.
- When the user binds ACL to an interface, TCAM resources will be consumed. One TCAM rule for each MAC or IP ACE and two TCAM rules for each IPv6 ACE.The TCAM consumption is always even number, so in case of odd number of rules the consumption will be increased by 1.

An ACL cannot be bound as input if it has been bound as output.

Example

```
switchxxxxxx(config)# mac access-list extended server-acl
switchxxxxxx(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
switchxxxxxx(config-mac-al)# exit
```

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# service-acl input server-acl default-action deny-any
```

4.11. service-acl output

Use the `service-acl output` command in Interface Configuration mode to control access to an interface on the egress (transmit path).

Use the no form of this command to remove the access control.

Syntax

- service-acl output acl-name1 [acl-name2]
- no service-acl output

Parameters

- acl-name-Specifies an ACL to apply to the interface. See the usage guidelines. (Range: acl-name is from 0-32 characters. Use "" for empty string)

Default

No ACL is assigned.

Command Mode

Interface Configuration mode(Ethernet, Port-Channel).

User Guidelines

The rule actions: log-input is not supported. Trying to use it will result in an error.

The deny rule action disable-port is not supported. Trying to use it will result in an error.

IPv4 and IPv6 ACLs can be bound together on an interface.

A MAC ACL cannot be bound on an interface together with an IPv4 ACL or IPv6 ACL.

Two ACLs of the same type cannot be added to a port.

An ACL cannot be added to a port that is already bounded to an ACL, without first removing the current ACL and binding the two ACLs together.

An ACL cannot be bound as output if it has been bound as input.

Example

This example binds an egress ACL to a port:

```
switchxxxxxx(config)# mac access-list extended server
switchxxxxxx(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
switchxxxxxx(config-mac-al)# exit
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# service-acl output server
```

4.12. time-range

Use the `time-range` Global Configuration mode command to define time ranges for different functions. In addition, this command enters the Time-range Configuration mode. All commands after this one refer to the time-range being defined.

This command sets a time-range name. Use the `absolute` and `periodic` commands to actually configure the time-range.

Use the no form of this command to remove the time range from the device.

Syntax

- time-range time-range-name
- no time-range time-range-name

Parameters

- time-range-name - Specifies the name for the time range. (Range: 1–32 characters)

Default Configuration

No time range is defined

Command Mode

Global Configuration mode

User Guidelines

After adding the name of a time range with this command, use the `absolute` and `periodic` commands to actually configure the time-range. Multiple periodic commands are allowed in a time range. Only one absolute command is allowed.

If a time-range command has both absolute and periodic values specified, then the periodic items are evaluated only after the absolute start time is reached, and are not evaluated again after the absolute end time is reached.

All time specifications are interpreted as local time.

To ensure that the time range entries take effect at the desired times, the software clock should be set by the user or by SNTP. If the software clock is not set by the user or by SNTP, the time range ACEs are not activated.

The user cannot delete a time-range that is bound to any features.

When a time range is defined, it can be used in the following commands:

- dot1x port-control
- power inline
- operation time
- permit (IP)
- deny (IP)
- permit (IPv6)
- deny (IPv6)
- permit (MAC)
- deny (MAC)

Example

```
switchxxxxxx(config)# time-range http-allowed
console(config-time-range)#periodic mon 12:00 to wed 12:00
```

4.13. absolute

Use the `absolute` Time-range Configuration mode command to specify an absolute time when a time range is in effect. Use the no form of this command to remove the time limitation.

Syntax

- absolute start hh:mm day month year
- no absolute start absolute end hh:mm day month year no absolute end

Parameters

- start - Absolute time and date that the permit or deny statement of the associated function going into effect. If no start time and date are specified, the function is in effect immediately.
- end - Absolute time and date that the permit or deny statement of the associated function is no longer in effect. If no end time and date are specified, the function is in effect indefinitely.
- hh:mm - Time in hours (military format) and minutes (Range: 0–23, mm: 0–5)
- day - Day (by date) in the month. (Range: 1–31)
- month - Month (first three letters by name). (Range: Jan...Dec)
- year - Year (no abbreviation) (Range: 2000–2097)

Default Configuration

There is no absolute time when the time range is in effect.

Command Mode

Time-range Configuration mode

User Guidelines

It is possible to define up to 10 absolute time-ranges.

Example

```
switchxxxxxx(config)# time-range http-allowed
switchxxxxxx(config-time-range)# absolute start 12:00 1 jan 2005
switchxxxxxx(config-time-range)# absolute end 12:00 31 dec 2005
```

4.14. periodic

Use the `periodic` Time-range Configuration mode command to specify a recurring (weekly) time range for functions that support the time-range feature. Use the no form of this command to remove the time limitation.

Syntax

- periodic day-of-the-week hh:mm to day-of-the-week hh:mm no periodic day-of-the-week hh:mm to day-of-the-week hh:mm periodic list hh:mm to hh:mm day-of-the-week1 [day-of-the-week2… day-of-the-week7]
- no periodic list hh:mm to hh:mm day-of-the-week1 [day-of-the-week2… day-of-the-week7] periodic list hh:mm to hh:mm all no periodic list hh:mm to hh:mm all

Parameters

- day-of-the-week - The starting day that the associated time range is in effect. The second occurrence is the ending day the associated statement is in effect. The second occurrence can be the following week (see description in the User Guidelines). Possible values are: mon, tue, wed, thu, fri, sat, and sun.
- hh:mm - The first occurrence of this argument is the starting hours:minutes (military format) that the associated time range is in effect. The second occurrence is the ending hours:minutes (military format) the associated statement is in effect. The second occurrence can be at the following day (see description in the User Guidelines). (Range: 0–23, mm: 0–59)
- list day-of-the-week1 - Specifies a list of days that the time range is in effect.

Default Configuration

There is no periodic time when the time range is in effect.

Command Mode

Time-range Configuration mode

User Guidelines

It is possible to define up to 10 periodic time-ranges.

The second occurrence of the day can be at the following week, e.g. Thursday– Monday means that the time range is effective on Thursday, Friday, Saturday, Sunday, and Monday.

The second occurrence of the time can be on the following day, e.g. “22:00–2:00”.

Example

```
switchxxxxxx(config)# time-range http-allowed
switchxxxxxx(config-time-range)# periodic mon 12:00 to wed 12:00
```

4.15. show time-range

Use the `show time-range` User EXEC mode command to display the time range configuration.

Syntax

- show time-range time-range-name

Parameters

- time-range-name - Specifies the name of an existing time range.

Command Mode

User EXEC mode

Example

```
switchxxxxxx> show time-range http-allowed -------------absolute start 12:00 1
Jan 2005 end 12:00 31 Dec 2005 periodic Monday 12:00 to Wednesday 12:00
```

4.16. show access-lists

Use the `show access-lists` Privileged EXEC mode command to display access control lists (ACLs) configured on the switch.

Syntax

- show access-lists [name]
- show access-liststime-range-active [name]

Parameters

- name - Specifies the name of the ACL.(Range: 1-160 characters).
- time-range-active - Shows only the Access Control Entries (ACEs) whose time-range is currently active (including those that are not associated with time-range).

Command Mode

Privileged EXEC mode

User Guidelines

The device can handle up to 2048 ACLs.

Example

```
switchxxxxxx# show access-lists Standard IP access list 1 Extended IP access
list ACL2 permit 234 172.30.19.1 0.0.0.255 any priority 20 time-range weekdays
permit 234 172.30.23.8 0.0.0.255 any priority 40 time-range weekdays
switchxxxxxx# show access-lists time-range-active Extended IP access list ACL1
permit 234 172.30.40.1 0.0.0.0 any priority 20 permit 234 172.30.8.8 0.0.0.0 any
priority 40 Extended IP access list ACL2 permit 234 172.30.19.1 0.0.0.255 any
priority 20time-range weekdays
switchxxxxxx# show access-lists ACL1
Extended IP access list ACL1 permit 234 172.30.40.1 0.0.0.0 any priority 20
permit 234 172.30.8.8 0.0.0.0 any priority 40
```

4.17. show interfaces access-lists

Use the `show interfaces access-lists` Privileged EXEC mode command to display access lists (ACLs) applied on interfaces.

Syntax

- show interfaces access-lists [interface-id]

Parameters

- interface-id - Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, port-channel or VLAN.

Command Mode

Privileged EXEC mode

Example

```
Interface ACLs
--------- ----------------------
te1/0/2 Ingress: server1
 Egress : ip
```

4.18. clear access-lists counters

Use the `clear access-lists counters` Privileged EXEC mode command to clear access-lists (ACLs) counters.

Syntax

- clear access-lists counters [interface-id]

Parameters

- interface-id - Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# clear access-lists counters te1/0/1
```

4.19. show interfaces access-lists trapped packets

Use the `show interfaces access-lists trapped packets` Privileged EXEC mode command to display Access List (ACLs) trapped packets.

Syntax

- show interfaces access-lists trapped packets [interface-id | port-channel-number | VLAN]

Parameters

- interface-id - Specifies an interface ID, the interface ID is an Ethernet port port-channel.
- port-channel - Specifies a port-channel.
- VLAN - Specifies a VLAN

Command Mode

Privileged EXEC mode

User Guidelines

This command shows whether packets were trapped from ACE hits with logging enable on an interface.

Examples

Example 1:

```
switchxxxxxx# show interfaces access-lists trapped packets
Ports/LAGs: te1/0/1-te1/0/3, ch1-ch3, ch4
VLANs: VLAN1, VLAN12-VLAN15
Packets were trapped globally due to lack of resources
```

Example 2:

```
switchxxxxxx# show interfaces access-lists trapped packets te1/0/1
Packets were trapped on interface te1/0/1
```

4.20. ip access-list (IP standard)

Use the `ip access-list` Global Configuration mode command to define an IP standard list. The no format of the command removes the list.

Syntax

- ip access-list access-list-name {deny|permit} {src-addr[/src-len] | any}
- no ip access-list access-list-name

Parameters

- access-list-name - The name of the Standard IP access list. The name may contain maximum 32 characters.
- deny/permit - Denies/permits access if the conditions are matched.
- src-addr[/src-len] | any - IP prefix defined as an IP address and length or any. The any value matches all IP addresses. If src-len is not defined, a value of 32 is applied. A value of src-len must be in the interval 1-32.

Default Configuration

No access list is defined.

Command Mode

Global Configuration mode

User Guidelines

Use the `ip access-list` command to configure IP address filtering. Access lists are configured with permit or deny keywords to either permit or deny an IP address based on a matching condition. An implicit deny is applied to address that does not match any access-list entry.

An access-list entry consists of an IP address and a bit mask. The bit mask is a number from 1 to 32.

Evaluation of an IP address by an access list starts with the first entry of the list and continues down the list until a match is found. When the IP address match is found, the permit or deny statement is applied to that address and the remainder of the list is not evaluated.

Use the no ip access-list command to delete the access list.

In addition to filtering IP traffic on a per port base, a basic IP access control list can be used by RIP (Routing Information Protocol) to filter route updates.

Examples

Example 1 - The following example of a standard access list allows only the three specified networks. Any IP address that does not match the access list statements will be rejected.

```
switchxxxxxx(config)# ip access-list 1 permit 192.168.34.0/24
switchxxxxxx(config)# ip access-list 1 permit 10.88.0.0/16
switchxxxxxx(config)# ip access-list 1 permit 10.0.0.0/8 Note: all other access
is implicitly denied.
```

Example 2 - The following example of a standard access list allows access for IP addresses in the range from 10.29.2.64 to 10.29.2.127. All IP addresses not in this range will be rejected.

```
switchxxxxxx(config)# ip access-list apo permit 10.29.2.64/26
Note: all other access is implicitly denied.
```

Example 3 - To specify a large number of individual addresses more easily, you can omit the mask length if it is 32. Thus, the following two configuration commands are identical in effect:

```
switchxxxxxx(config)# ip access-list 2aa permit 10.48.0.3
switchxxxxxx(config)# ip access-list 2aa permit 10.48.0.3/32
```

4.21. ipv6 access-list (IP standard)

The `ipv6 access-list` Global Configuration mode command defines an IPv6 standard list. The no format of the command removes the list.

Syntax

- ipv6 access-list access-list-name {deny|permit} {src-addr[/src-len] | any}
- no ipv6 access-list access-list-name

Parameters

- access-list-name - The name of the Standard IPv6 access list. The name may contain maximum 32 characters.
- deny - Denies access if the conditions are matched.
- permit - Permits access if the conditions are matched.

- src-addr[/src-len] | any - IPv6 prefix defined as an IPv6 address and length or any. The any value matches to all IPv6 addresses. If the src-len is not defined a value of 128 is applied. A value of src-len must be in interval 1-128.

Default Configuration

no access list

Command Mode

Global Configuration mode

User Guidelines

Use the `ipv6 access-list` command to configure IPv6 address filtering. Access lists are configured with permit or deny keywords to either permit or deny an IPv6 address based on a matching condition. An implicit deny is applied to address that does not match any access-list entry.

An access-list entry consists of an IP address and a bit mask. The bit mask is a number from 1 to 128.

Evaluation of an IPv6 address by an access list starts with the first entry of the list and continues down the list until a match is found. When the IPv6 address match is found, the permit or deny statement is applied to that address and the remainder of the list is not evaluated.

Use the no ipv6 access-list command to delete the access list.

The IPv6 standard access list is used to filter received and sent IPv6 routing information.

Example

The following example of an access list allows only the one specified prefix: Any IPv6 address that does not match the access list statements will be rejected.

```
switchxxxxxx(config)# ipv6 access-list 1 permit 3001::2/64
Note: all other access implicitly denied.
```

5. Address Table Commands

5.1. bridge multicast filtering

To enable the filtering of Multicast addresses, use the `bridge multicast filtering` Global Configuration mode command. To disable Multicast address filtering, use the no form of this command.

Syntax

- bridge multicast filtering
- no bridge multicast filtering

Parameters

This command has no arguments or keywords.

Default Configuration

Multicast address filtering is disabled. All Multicast addresses are flooded to all ports.

Command Mode

Global Configuration mode

User Guidelines

When this feature is enabled, unregistered Multicast traffic (as opposed to registered) will still be flooded.

All registered Multicast addresses will be forwarded to the Multicast groups. There are two ways to manage Multicast groups, one is the IGMP Snooping feature, and the other is the `bridge multicast forward-all` command.

Example

The following example enables bridge Multicast filtering.

```
switchxxxxxx(config)# bridge multicast filtering
```

5.2. bridge multicast mode

To configure the Multicast bridging mode, use the `bridge multicast mode` Interface (VLAN) Configuration mode command. To return to the default configuration, use the no form of this command.

Syntax

- bridge multicast mode {mac-group | ipv4-group | ipv4-src-group}
- no bridge multicast mode

Parameters

- mac-group - Specifies that Multicast bridging is based on the packet's VLAN and MAC address.
- ipv4-group - Specifies that Multicast bridging is based on the packet's VLAN and MAC address for non-IPv4 packets, and on the packet's VLAN and IPv4 destination address for IPv4 packets.
- ipv4-src-group - Specifies that Multicast bridging is based on the packet's VLAN and MAC address for non-IPv4 packets, and on the packet's VLAN, IPv4 destination address and IPv4 source address for IPv4 packets.

Default Configuration

The default mode is mac-group.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use the mac-group option when using a network management system that uses a MIB based on the Multicast MAC address. Otherwise, it is recommended to use the ipv4 mode, because there is no overlapping of IPv4 Multicast addresses in these modes.

For each Forwarding Data Base (FDB) mode, use different CLI commands to configure static entries in the FDB, as described in the following table:

FDB Mode		CLI Commands
mac-group	bridge multicast address	bridge multicast forbidden address
ipv4-group	bridge multicast ip-address	bridge multicast forbidden ip-addresss
ipv4-src-group	bridge multicast source group	bridge multicast forbidden source group

The following table describes the actual data that is written to the Forwarding Data Base (FDB) as a function of the IGMP version that is used in the network:

FDB mode	IGMP version 2	IGMP version 3
mac-group	MAC group address	MAC group address
ipv4-group	IP group address	IP group address
ipv4-src-group	(*)	IP source and group addresses

(*) Note that (*,G) cannot be written to the FDB if the mode is ipv4-src-group. In that case, no new FDB entry is created, but the port is added to the static (S,G) entries (if they exist) that belong to the requested group. It is recommended to set the FDB mode to ipv4-group or mac-group for IGMP version 2.

If an application on the device requests (*,G), the operating FDB mode is changed to ipv4-group.

Example

The following example configures the Multicast bridging mode as an mac-group on VLAN 2.

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# bridge multicast mode mac-group
```

5.3. bridge multicast address

To register a MAC-layer Multicast address in the bridge table and statically add or remove ports to or from the group, use the `bridge multicast address` Interface (VLAN) Configuration mode command. To unregister the MAC address, use the no form of this command.

Syntax

- bridge multicast address {mac-multicast-address | ipv4-multicast-address} [{add | remove} {ethernet interface-list | port-channel port-channel-list}]
- no bridge multicast address mac-multicast-address

Parameters

- mac-multicast-address | ipv4-multicast-address - Specifies the group Multicast address.
- add - (Optional) Adds ports to the group.
- remove - (Optional) Removes ports from the group.
- ethernet interface-list - (Optional) Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- port-channel port-channel-list - (Optional) Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

Default Configuration

No Multicast addresses are defined.

If ethernet interface-list or port-channel port-channel-list is specified without specifying add or remove, the default option is add.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

To register the group in the bridge database without adding or removing ports or port channels, specify the mac-multicast-address parameter only.

Static Multicast addresses can be defined on static VLANs only.

You can execute the command before the VLAN is created.

Examples

Example 1 - The following example registers the MAC address to the bridge table:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast address 01:00:5e:02:02:03
```

Example 2 - The following example registers the MAC address and adds ports statically.

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast address 01:00:5e:02:02:03 add te1/0/1-
2
```

5.4. bridge multicast forbidden address

To forbid adding or removing a specific Multicast address to or from specific ports, use the `bridge multicast forbidden address` Interface (VLAN) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- bridge multicast forbidden address {mac-multicast-address | ipv4-multicast-address} {add | remove} {ethernet interface-list | port-channel port-channel-list}

- no bridge multicast forbidden address mac-multicast-address

Parameters

- mac-multicast-address | ipv4-multicast-address - Specifies the group Multicast address.
- add - Forbids adding ports to the group.
- remove - Forbids removing ports from the group.
- ethernet interface-list - Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- port-channel port-channel-list - Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

No forbidden addresses are defined.

Default option is add.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Before defining forbidden ports, the Multicast group should be registered, using `bridge multicast address`.

You can execute the command before the VLAN is created.

Example

The following example forbids MAC address 0100.5e02.0203 on port te1/0/4 within VLAN 8.

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast address 0100.5e02.0203
switchxxxxxx(config-if)# bridge multicast forbidden address 0100.5e02.0203 add
te1/0/4
```

5.5. bridge multicast ip-address

To register IP-layer Multicast addresses to the bridge table, and statically add or remove ports to or from the group, use the `bridge multicast ip-address` IInterface (VLAN) Configuration mode command. To unregister the IP address, use the no form of this command.

Syntax

- bridge multicast ip-address ip-multicast-address [[add | remove] {interface-list | port-channel port-channel-list}]
- no bridge multicast ip-address ip-multicast-address

Parameters

- ip-multicast-address - Specifies the group IP Multicast address.
- add - (Optional) Adds ports to the group.
- remove - (Optional) Removes ports from the group.
- interface-list - (Optional) Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.

- port-channel port-channel-list - (Optional) Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

No Multicast addresses are defined.

Default option is add.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

To register the group in the bridge database without adding or removing ports or port channels, specify the ip-multicast-address parameter only.

Static Multicast addresses can be defined on static VLANs only.

You can execute the command before the VLAN is created.

Example

The following example registers the specified IP address to the bridge table:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast ip-address 239.2.2.2
```

The following example registers the IP address and adds ports statically.

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast ip-address 239.2.2.2 add te1/0/4
```

5.6. bridge multicast forbidden ip-address

To forbid adding or removing a specific IP Multicast address to or from specific ports, use the `bridge multicast forbidden ip-address` Interface (VLAN) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- bridge multicast forbidden ip-address {ip-multicast-address} {add | remove} {ethernet interface-list | port-channel port-channel-list}
- no bridge multicast forbidden ip-address ip-multicast-address

Parameters

- ip-multicast-address - Specifies the group IP Multicast address.
- add - (Optional) Forbids adding ports to the group.
- remove - (Optional) Forbids removing ports from the group.
- ethernet interface-list - (Optional) Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- port-channel port-channel-list - (Optional) Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

No forbidden addresses are defined.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Before defining forbidden ports, the Multicast group should be registered.

You can execute the command before the VLAN is created.

Example

The following example registers IP address 239.2.2.2, and forbids the IP address on port te1/0/4 within VLAN 8.

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast ip-address 239.2.2.2
switchxxxxxx(config-if)# bridge multicast forbidden ip-address 239.2.2.2 add
te1/0/4
```

5.7. bridge multicast source group

To register a source IP address - Multicast IP address pair to the bridge table, and statically add or remove ports to or from the source-group, use the `bridge multicast source group` Interface (VLAN) Configuration mode command. To unregister the source-group-pair, use the no form of this command.

Syntax

- bridge multicast source ip-address group ip-multicast-address [[add | remove] {ethernet interface-list | port-channel port-channel-list}]
- no bridge multicast source ip-address group ip-multicast-address

Parameters

- ip-address - Specifies the source IP address.
- ip-multicast-address - Specifies the group IP Multicast address.
- add - (Optional) Adds ports to the group for the specific source IP address.
- remove - (Optional) Removes ports from the group for the specific source IP address.
- ethernet interface-list - (Optional) Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- port-channel port-channel-list - (Optional) Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

Default Configuration

No Multicast addresses are defined.

The default option is add.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

You can execute the command before the VLAN is created.

Example

The following example registers a source IP address - Multicast IP address pair to the bridge table:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast source 13.16.1.1 group 239.2.2.2
```

5.8. bridge multicast forbidden source group

To forbid adding or removing a specific IP source address - Multicast address pair to or from specific ports, use `the bridge multicast forbidden source group` Interface (VLAN) Configuration mode command. To return to the default configuration, use the no form of this command.

Syntax

- bridge multicast forbidden source ip-address group ip-multicast-address {add | remove} {ethernet interface-list | port-channel port-channel-list}
- no bridge multicast forbidden source ip-address group ip-multicast-address

Parameters

- ip-address - Specifies the source IP address.
- ip-multicast-address - Specifies the group IP Multicast address.
- add - (Optional) Forbids adding ports to the group for the specific source IP address.
- remove - (Optional) Forbids removing ports from the group for the specific source IP address.
- ethernet interface-list - (Optional) Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- port-channel port-channel-list - (Optional) Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

Default Configuration

No forbidden addresses are defined.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Before defining forbidden ports, the Multicast group should be registered.

You can execute the command before the VLAN is created.

Example

The following example registers a source IP address - Multicast IP address pair to the bridge table, and forbids adding the pair to port te1/0/4 on VLAN 8:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast source 13.16.1.1 group 239.2.2.2
switchxxxxxx(config-if)# bridge multicast forbidden source 13.16.1.1 group
239.2.2.2 add te1/0/4
```

5.9. bridge multicast ipv6 mode

To configure the Multicast bridging mode for IPv6 Multicast packets, use the `bridge multicast ipv6 mode` Interface (VLAN) Configuration mode command. To return to the default configuration, use the no form of this command.

Syntax

- bridge multicast ipv6 mode {mac-group | ip-group | ip-src-group}
- no bridge multicast ipv6 mode

Parameters

- mac-group - Specifies that Multicast bridging is based on the packet's VLAN and MAC destination address.
- ip-group - Specifies that Multicast bridging is based on the packet's VLAN and IPv6 destination address for IPv6 packets.
- ip-src-group - Specifies that Multicast bridging is based on the packet's VLAN, IPv6 destination address and IPv6 source address for IPv6 packets.

Default Configuration

The default mode is mac-group.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use the mac-group mode when using a network management system that uses a MIB based on the Multicast MAC address.

For each Forwarding Data Base (FDB) mode, use different CLI commands to configure static entries for IPv6 Multicast addresses in the FDB, as described in the following table::

FDB Mode	CLI Commands
mac-group	bridge multicast address bridge multicast forbidden address
ipv6-group	bridge multicast ipv6 bridge multicast ipv6 ip-address forbidden ip-address
ipv6-src-grou p	bridge multicast ipv6 source bridge multicast ipv6 group forbidden source group

The following table describes the actual data that is written to the Forwarding Data Base (FDB) as a function of the MLD version that is used in the network:

FDB mode	MLD version 1	MLD version 2
mac-group	MAC group address	MAC group address
ipv6-group	IPv6 group address	IPv6 group address
ipv6-src-group	(*)	IPv6 source and group addresses

(*) In ip-src-group mode a match is performed on 4 bytes of the multicast address and 4 bytes of the source address. In the group address the last 4 bytes of the address are checked for match. In the source address the last 3 bytes and 5th from last bytes of the interface ID are examined.

(*) Note that (*,G) cannot be written to the FDB if the mode is ip-src-group. In that case, no new FDB entry is created, but the port is added to the (S,G) entries (if they exist) that belong to the requested group.

If an application on the device requests (*,G), the operating FDB mode is changed to ip-group.

You can execute the command before the VLAN is created.

Example

The following example configures the Multicast bridging mode as an ip-group on VLAN 2.

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# bridge multicast ipv6 mode ip-group
```

5.10. bridge multicast ipv6 ip-address

To register an IPv6 Multicast address to the bridge table, and statically add or remove ports to or from the group, use the `bridge multicast ipv6 ip-address` Interface (VLAN) Configuration mode command. To unregister the IPv6 address, use the no form of this command.

Syntax

- bridge multicast ipv6 ip-address ipv6-multicast-address [[add | remove] {ethernet interface-list | port-channel port-channel-list}]
- no bridge multicast ipv6 ip-address ip-multicast-address

Parameters

- ipv6-multicast-address - Specifies the group IPv6 multicast address.
- add - (Optional) Adds ports to the group.
- remove - (Optional) Removes ports from the group.
- ethernet interface-list - (Optional) Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces; use a hyphen to designate a range of ports.
- port-channel port-channel-list - (Optional) Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

No Multicast addresses are defined.

The default option is add.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

To register the group in the bridge database without adding or removing ports or port channels, specify the ipv6-multicast-address parameter only.

Static Multicast addresses can be defined on static VLANs only.

You can execute the command before the VLAN is created.

Examples

Example 1 - The following example registers the IPv6 address to the bridge table:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast ipv6 ip-address FF00:0:0:0:4:4:4:1
```

Example 2 - The following example registers the IPv6 address and adds ports statically.

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast ipv6 ip-address FF00:0:0:0:4:4:4:1 add
te1/0/1-2
```

5.11. bridge multicast ipv6 forbidden ip-address

To forbid adding or removing a specific IPv6 Multicast address to or from specific ports, use the `bridge multicast ipv6 forbidden ip-address` Interface (VLAN) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- bridge multicast ipv6 forbidden ip-address {ipv6-multicast-address} {add | remove} {ethernet interface-list | port-channel port-channel-list}
- no bridge multicast ipv6 forbidden ip-address ipv6-multicast-address

Parameters

- ipv6-multicast-address - Specifies the group IPv6 Multicast address.
- add - (Optional) Forbids adding ports to the group.
- remove - (Optional) Forbids removing ports from the group.
- ethernet interface-list - (Optional) Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- port-channel port-channel-list - (Optional) Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

No forbidden addresses are defined.

The default option is add.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Before defining forbidden ports, the Multicast group should be registered.

You can execute the command before the VLAN is created.

Example

The following example registers an IPv6 Multicast address, and forbids the IPv6 address on port te1/0/4 within VLAN 8.

```
switchxxxxxx(config)# interface vlan 8
```

```
switchxxxxxx(config-if)# bridge multicast ipv6 ip-address FF00:0:0:0:4:4:4:1
switchxxxxxx(config-if)# bridge multicast ipv6 forbidden ip-address
FF00:0:0:0:4:4:4:1 add te1/0/4
```

5.12. bridge multicast ipv6 source group

To register a source IPv6 address - Multicast IPv6 address pair to the bridge table, and statically add or remove ports to or from the source-group, use the `bridge multicast ipv6 source group` Interface (VLAN) Configuration mode command. To unregister the source-group-pair, use the no form of this command.

Syntax

- bridge multicast ipv6 source ipv6-source-address group ipv6-multicast-address [[add | remove] {ethernet interface-list | port-channel port-channel-list}]
- no bridge multicast ipv6 source ipv6-address group ipv6-multicast-address

Parameters

- ipv6-source-address - Specifies the source IPv6 address.
- ipv6-multicast-address - Specifies the group IPv6 Multicast address.
- add - (Optional) Adds ports to the group for the specific source IPv6 address.
- remove - (Optional) Removes ports from the group for the specific source IPv6 address.
- ethernet interface-list - (Optional) Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- port-channel port-channel-list - (Optional) Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

No Multicast addresses are defined.

The default option is add.

Command Mode

Interface (VLAN) Configuration mode

Example

The following example registers a source IPv6 address - Multicast IPv6 address pair to the bridge table:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast source 2001:0:0:0:4:4:4 group
FF00:0:0:0:4:4:4:1
```

5.13. bridge multicast ipv6 forbidden source group

To forbid adding or removing a specific IPv6 source address - Multicast address pair to or from specific ports, use the `bridge multicast ipv6 forbidden source group` Interface (VLAN) Configuration mode command. To return to the default configuration, use the no form of this command.

Syntax

- bridge multicast ipv6 forbidden source ipv6-source-address group ipv6-multicast-address {add | remove} {ethernet interface-list | port-channel port-channel-list}
- no bridge multicast ipv6 forbidden source ipv6-address group ipv6-multicast-address

Parameters

- ipv6-source-address - Specifies the source IPv6 address.
- ipv6-multicast-address - Specifies the group IPv6 Multicast address.
- add - Forbids adding ports to the group for the specific source IPv6 address.
- remove - Forbids removing ports from the group for the specific source IPv6 address.
- ethernet interface-list - Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- port-channel port-channel-list - Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

Default Configuration

No forbidden addresses are defined.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Before defining forbidden ports, the Multicast group should be registered.

You can execute the command before the VLAN is created.

Example

The following example registers a source IPv6 address - Multicast IPv6 address pair to the bridge table, and forbids adding the pair to te1/0/4 on VLAN 8:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast source 2001:0:0:0:4:4:4 group
FF00:0:0:0:4:4:4:1
switchxxxxxx(config-if)# bridge multicast forbidden source 2001:0:0:0:4:4:4:1
group FF00:0:0:0:4:4:4:1 add te1/0/4
```

5.14. bridge multicast unregistered

To configure forwarding unregistered Multicast addresses, use the `bridge multicast unregistered` Interface (Ethernet, Port Channel) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- bridge multicast unregistered {forwarding | filtering}
- no bridge multicast unregistered

Parameters

- forwarding - Forwards unregistered Multicast packets.
- filtering - Filters unregistered Multicast packets.

Default Configuration

Unregistered Multicast addresses are forwarded.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Do not enable unregistered Multicast filtering on ports that are connected to routers, because the 224.0.0.x address range should not be filtered. Note that routers do not necessarily send IGMP reports for the 224.0.0.x range.

You can execute the command before the VLAN is created.

Example

The following example specifies that unregistered Multicast packets are filtered on te1/0/1:

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# bridge multicast unregistered filtering
```

5.15. bridge multicast forward-all

To enable forwarding all multicast packets for a range of ports or port channels, use the `bridge multicast forward-all` Interface (VLAN) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- bridge multicast forward-all {add | remove} {ethernet interface-list | port-channel port-channel-list}
- no bridge multicast forward-all

Parameters

- add - Forces forwarding of all Multicast packets.
- remove - Does not force forwarding of all Multicast packets.
- ethernet interface-list - Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- port-channel port-channel-list - Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

Forwarding of all Multicast packets is disabled.

Command Mode

Interface (VLAN) Configuration mode

Example

The following example enables all Multicast packets on port te1/0/4 to be forwarded.

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# bridge multicast forward-all add te1/0/4
```

5.16. bridge multicast forbidden forward-all

To forbid a port to dynamically join Multicast groups, use the `bridge multicast forbidden forward-all` Interface (VLAN) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- bridge multicast forbidden forward-all {add | remove} {ethernet interface-list | port-channel port-channel-list}
- no bridge multicast forbidden forward-all

Parameters

- add - Forbids forwarding of all Multicast packets.
- remove - Does not forbid forwarding of all Multicast packets.
- ethernet interface-list - Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- port-channel port-channel-list - Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

Default Configuration

Ports are not forbidden to dynamically join Multicast groups.

The default option is add.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use this command to forbid a port to dynamically join (by IGMP, for example) a Multicast group.

The port can still be a Multicast router port.

Example

The following example forbids forwarding of all Multicast packets to te1/0/1 within VLAN 2.

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# bridge multicast forbidden forward-all add ethernet
te1/0/1
```

5.17. bridge unicast unknown

To enable egress filtering of Unicast packets where the destination MAC address is unknown to the device, use the `bridge unicast unknown` Interface (Ethernet, Port Channel) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- bridge unicast unknown {filtering | forwarding}
- no bridge unicast unknown

Parameters

- filtering - Filter unregistered Unicast packets.
- forwarding - Forward unregistered Unicast packets.

Default Configuration

Forwarding.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode.

Example

The following example drops Unicast packets on te1/0/1 when the destination is unknown.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# bridge unicast unknown filtering
```

5.18. show bridge unicast unknown

To display the unknown Unicast filtering configuration, use the `show bridge unicast unknown` Privileged EXEC mode command.

Syntax

- show bridge unicast unknown [interface-id]

Parameters

- interface-id - (Optional) Specify an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel

Command Mode

Privileged EXEC mode

Example

```
Console # show bridge unicast unknown
Port Unregistered
------- ---------------------
te1/0/1 Forward
te1/0/2 Filter
te1/0/3 Filter
```

5.19. mac address-table static

To add a MAC-layer station source address to the MAC address table, use the `mac address-table static` Global Configuration mode command. To delete the MAC address, use the no form of this command.

Syntax

- mac address-table static mac-address vlan vlan-id interface interface-id [permanent | delete-on-reset | delete-on-timeout | secure]|
- no mac address-table static [mac-address] vlan vlan-id

Parameters

- mac-address - MAC address (Range: Valid MAC address)
- vlan-id - Specify the VLAN

- interface-id - Specify an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel (Range: valid ethernet port, valid port-channel)
- permanent - (Optional) The permanent static MAC address. The keyword is applied by the default.
- delete-on-reset - (Optional)The delete-on-reset static MAC address.
- delete-on-timeout - (Optional)The delete-on-timeout static MAC address.
- secure - (Optional)The secure MAC address. May be used only in a secure mode.

Default Configuration

No static addresses are defined. The default mode for an added address is permanent.

The MAC table size is 16 k.

Command Mode

Global Configuration mode

User Guidelines

Use the command to add a static MAC address with given time-to-live in any mode or to add a secure MAC address in a secure mode.

Each MAC address in the MAC address table is assigned two attributes: type and time-to-live.

The following value of time-of-live is supported:

- permanent - MAC address is saved until it is removed manually.
- delete-on-reset - MAC address is saved until the next reboot.
- delete-on-timeout - MAC address that may be removed by the aging timer. The following types are supported:
  - static - MAC address manually added by the command with the following keywords specifying its time-of-live:
  - permanent
  - delete-on-reset
  - delete-on-timeout

    A static MAC address may be added in any port mode.

  - secure - A MAC address added manually or learned in a secure mode. Use the mac address-table static command with the secure keyword to add a secure MAC address. The MAC address cannot be relearned.

    A secure MAC address may be added only in a secure port mode.
- dynamic - a MAC address learned by the switch in non-secure mode. A value of its time-to-live attribute is delete-on-timeout.

Examples

Example 1 - The following example adds two permanent static MAC address:

```
switchxxxxxx(config)# mac address-table static 00:3f:bd:45:5a:b1 vlan 1
interface te1/0/1
switchxxxxxx(config)# mac address-table static 00:3f:bd:45:5a:b2 vlan 1
interface te1/0/1 permanent
```

Example 2 - The following example adds a deleted-on-reset static MAC address:

```
switchxxxxxx(config)# mac address-table static 00:3f:bd:45:5a:b2 vlan 1
interface te1/0/1 delete-on-reset
```

Example 3 - The following example adds a deleted-on-timeout static MAC address:

```
switchxxxxxx(config)# mac address-table static 00:3f:bd:45:5a:b2 vlan 1
interface te1/0/1 delete-on-timeout
```

Example 4 - The following example adds a secure MAC address:

```
switchxxxxxx(config)# mac address-table static 00:3f:bd:45:5a:b2 vlan 1
interface te1/0/1 secure
```

5.20. clear mac address-table

To remove learned or secure entries from the forwarding database (FDB), use the `clear mac address-table` Privileged EXEC mode command.

Syntax

clear mac address-table dynamic interface interface-id clear mac address-table secure interface interface-id

Parameters

- dynamic interface interface-id - Delete all dynamic (learned) addresses on the specified interface.The interface ID can be one of the following types: Ethernet port or port-channel. If interface ID is not supplied, all dynamic addresses are deleted.
- secure interface interface-id - Delete all the secure addresses learned on the specific interface. A secure address on a MAC address learned on ports on which port security is defined.

Default Configuration

For dynamic addresses, if interface-id is not supplied, all dynamic entries are deleted.

Command Mode

Privileged EXEC mode

Examples

Example 1 - Delete all dynamic entries from the FDB.

```
switchxxxxxx# clear mac address-table dynamic
```

Example 2 - Delete all secure entries from the FDB learned on secure port te1/0/1.

```
switchxxxxxx# clear mac address-table secure interface te1/0/1
```

5.21. mac address-table aging-time

To set the aging time of the address table, use the `mac address-table aging-time` Global configuration command. To restore the default, use the no form of this command.

Syntax

- mac address-table aging-time seconds
- no mac address-table aging-time

Parameters

- seconds - Time is number of seconds. (Range:10-630)

Default Configuration

300

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# mac address-table aging-time 600
```

5.22. port security

To enable port security learning mode on an interface, use the `port security` Interface (Ethernet, Port Channel) Configuration mode command. To disable port security learning mode on an interface, use the no form of this command.

Syntax

- port security [forward | discard | discard-shutdown] [trap seconds]
- no port security

Parameters

- forward - (Optional) Forwards packets with unlearned source addresses, but does not learn the address.
- discard - (Optional) Discards packets with unlearned source addresses.
- discard-shutdown - (Optional) Discards packets with unlearned source addresses and shuts down the port.
- trap seconds - (Optional) Sends SNMP traps and specifies the minimum time interval in seconds between consecutive traps. (Range: 1–1000000)

Default Configuration

The feature is disabled by default.

The default mode is discard.

The default number of seconds is zero, but if traps is entered, a number of seconds must also be entered.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The command may be used only when the interface in the regular (non-secure with unlimited MAC learning) mode.

See the `mac address-table static` command for information about MAC address attributes (type and time-to-live) definitions.

When the port security command enables the lock mode on a port all dynamic addresses learned on the port are changed to permanent secure addresses.

When the port security command enables a mode on a port differing from the lock mode all dynamic addresses learned on the port are deleted.

When the no port security command cancels a secure mode on a port all secure addresses defined on the port are changed to dynamic addresses.

Additionally to set a mode, use the `port security` command to set an action that the switch should perform on a frame which source MAC address cannot be learned.

Example

The following example forwards all packets to port te1/0/1 without learning addresses of packets from unknown sources and sends traps every 100 seconds, if a packet with an unknown source address is received.

```
switchxxxxxx(config)# interface te1/0/4
switchxxxxxx(config-if)# port security mode lock
switchxxxxxx(config-if)# port security forward trap 100
switchxxxxxx(config-if)# exit
```

5.23. port security mode

To configure the port security learning mode, use the `port security mode` Interface (Ethernet, Port Channel) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- port security mode {max-addresses | lock | secure permanent | secure delete-on-reset}
- no port security mode

Parameters

- max-addresses - Non-secure mode with limited learning dynamic MAC addresses. Up to 1024 static MAC addresses may be added on the port manually by the `mac address-table static` command.
- lock - Secure mode without MAC learning. The static and secure MAC addresses may be added on the port manually by the `mac address-table static` command.
- secure permanent - Secure mode with limited learning permanent secure MAC addresses with the permanent time-of-live. The static and secure MAC addresses may be added on the port manually by the mac address-table static command.
- secure delete-on-reset - Secure mode with limited learning secure MAC addresses with the delete-on-reset time-of-live. The static and secure MAC addresses may be added on the port manually by the mac address-table static command.

Default Configuration

The default port security mode is lock.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The default port mode is called regular. In this mode, the port allows unlimited learning of dynamic addresses.

The static MAC addresses may be added on the port manually by the `mac address-table static` command.

The command may be used only when the interface in the regular (non-secure with unlimited MAC learning) mode.

Use the `port security mode` command to change the default mode before the `port security` command.

Example

The following example sets the port security mode to Lock for te1/0/4.

```
switchxxxxxx(config)# interface te1/0/4
switchxxxxxx(config-if)# port security mode lock
switchxxxxxx(config-if)# port security
switchxxxxxx(config-if)# exit
```

5.24. port security max

To configure the maximum number of addresses that can be learned on the port while the port is in port, max-addresses or secure mode, use the `port security max` Interface (Ethernet, Port Channel) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- port security max max-addr
- no port security max

Parameters

- max-addr - Specifies the maximum number of addresses that can be learned on the port. (Range: 0–256)

Default Configuration

This default maximum number of addresses is 1.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The command may be used only when the interface in the regular (non-secure with unlimited MAC learning) mode.

Use this command to change the default value before the `port security` command.

Example

The following example sets the port to limited learning mode:

```
switchxxxxxx(config)# interface te1/0/4
switchxxxxxx(config-if)# port security mode max
switchxxxxxx(config-if)# port security max 20
switchxxxxxx(config-if)# port security
switchxxxxxx(config-if)# exit
```

5.25. port security routed secure-address

To add a MAC-layer secure address to a routed port. (port that has an IP address defined on it), use the `port security routed secure-address` Interface (Ethernet, Port

Channel) Configuration mode command. To delete a MAC address from a routed port, use the no form of this command.

Syntax

- port security routed secure-address mac-address
- no port security routed secure-address mac-address

Parameters

- mac-address - Specifies the MAC address.

Default Configuration

No addresses are defined.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode. It cannot be configured for a range of interfaces (range context).

User Guidelines

This command enables adding secure MAC addresses to a routed port in port security mode. The command is available when the port is a routed port and in port security mode. The address is deleted if the port exits the security mode or is not a routed port.

Example

The following example adds the MAC-layer address 00:66:66:66:66:66 to te1/0/1.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# port security routed secure-address 00:66:66:66:66:66
```

5.26. show mac address-table

To display entries in the MAC address table, use the `show mac address-table` Privileged EXEC mode command.

Syntax

- show mac address-table [dynamic | static | secure] [vlan vlan] [interface interface-id] [address mac-address]

Parameters

- dynamic - (Optional) Displays only dynamic MAC address table entries.
- static - (Optional) Displays only static MAC address table entries.
- secure - (Optional) Displays only secure MAC address table entries.
- vlan - (Optional) Displays entries for a specific VLAN.
- interface interface-id - (Optional) Displays entries for a specific interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- address mac-address - (Optional) Displays entries for a specific MAC address.

Default Configuration

If no parameters are entered, the entire table is displayed.

Command Mode

Privileged EXEC mode

User Guidelines

Internal usage VLANs (VLANs that are automatically allocated on routed ports) are presented in the VLAN column by a port number and not by a VLAN ID.

Examples

Example 1 - Displays entire address table.

```
switchxxxxxx# show mac address-table
Aging time is 300 sec
      VLAN  MAC Address Port  Type
      --------    ---------------------   ----------  ----------
      1     00:00:26:08:13:23 0     self
      1     00:3f:bd:45:5a:b1 te1/0/1     static
1 00:a1:b0:69:63:f3 te1/0/2 dynamic 2 00:a1:b0:69:63:f3 te1/0/3 dynamic te1/0/4
00:a1:b0:69:61:12 te1/0/4 dynamic
```

Example 2 - Displays address table entries containing the specified MAC address.

```
switchxxxxxx# show mac address-table address 00:3f:bd:45:5a:b1
Aging time is 300 sec
VLAN MAC Address Port Type
-------- --------------------- ---------- ----------
1 00:3f:bd:45:5a:b1 static te1/0/4
```

5.27. show mac address-table count

To display the number of addresses present in the Forwarding Database, use the `show mac address-table count` Privileged EXEC mode command.

Syntax

- show mac address-table count [vlan vlan | interface interface-id]

Parameters

- vlan vlan - (Optional) Specifies VLAN.
- interface-id interface-id - (Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show mac address-table count
This may take some time.
Capacity : 16384
Free : 16379
Used : 5
Secure : 0
Dynamic : 2
Static : 2 Internal : 1 console#
```

5.28. show bridge multicast mode

To display the Multicast bridging mode for all VLANs or for a specific VLAN, use the `show bridge multicast mode` Privileged EXEC mode command.

Syntax

- show bridge multicast mode [vlan vlan-id]

Parameters

- vlan vlan-id - (Optional) Specifies the VLAN ID.

Command Mode

Privileged EXEC mode

Example

The following example displays the Multicast bridging mode for all VLANs

```
switchxxxxxx# show bridge multicast mode
VLAN IPv4 Multicast Mode IPv6 Multicast Mode
 Admin Oper Admin Oper
---- -------- --------- ------- -----------
1 MAC-GROUP MAC-GROUP MAC-GROUP MAC-GROUP
11 IPv4-GROUP IPv4-GROUP IPv6-GROUP IPv6-GROUP
12 IPv4-SRC-GROUP IPv4-SRC-GROUP IPv6-SRC-GROUP IPv6-SRC-GROUP
```

5.29. show bridge multicast address-table

To display Multicast MAC addresses or IP Multicast address table information, use the `show bridge multicast address-table` Privileged EXEC mode command.

Syntax

- show bridge multicast address-table [vlan vlan-id]
- show bridge multicast address-table [vlan vlan-id] [address mac-multicast-address] [format {ip | mac}]
- show bridge multicast address-table [vlan vlan-id] [address ipv4-multicast-address] [source ipv4-source-address]
- show bridge multicast address-table [vlan vlan-id] [address ipv6-multicast-address] [source ipv6-source-address]

Parameters

- vlan-id vlan-id - (Optional) Display entries for specified VLAN ID.
- address - (Optional) Display entries for specified Multicast address. The possible values are:
  - mac-multicast-address - (Optional) Specifies the MAC Multicast address.
  - ipv4-multicast-address - (Optional) Specifies the IPv4 Multicast address.
  - ipv6-multicast-address - (Optional) Specifies the IPv6 Multicast address.
- format - (Optional) Applies if mac-multicast-address was selected. In this case either MAC or IP format can be displayed. Display entries for specified Multicast address format. The possible values are:
  - ip - Specifies that the Multicast address is an IP address.
  - mac - Specifies that the Multicast address is a MAC address.
- source - (Optional) Specifies the source address. The possible values are:
  - ipv4-address - (Optional) Specifies the source IPv4 address.
  - ipv6-address - (Optional) Specifies the source IPv6 address.

Default Configuration

If the format is not specified, it defaults to mac (only if mac-multicast-address was entered).

If VLAN ID is not entered, entries for all VLANs are displayed.

If MAC or IP address is not supplied, entries for all addresses are displayed.

Command Mode

Privileged EXEC mode

User Guidelines

A MAC address can be displayed in IP format only if it is within the range 0100.5e00.0000 through 0100.5e7f.ffff.

Multicast router ports (defined statically or discovered dynamically) are members in all MAC groups.

Ports that were defined via the `bridge multicast forbidden forward-all` command are displayed in all forbidden MAC entries.

Changing the Multicast mode can move static Multicast addresses that are written in the device FDB to a shadow configuration because of FDB hash collisions.

Example

The following example displays bridge Multicast address information.

```
switchxxxxxx# show bridge multicast address-table
Multicast address table for VLANs in MAC-GROUP bridging mode:
Vlan MAC Address Type Ports
---- ----------------- -------------- ----- 8 01:00:5e:02:02:03 Static 1-2
Forbidden ports for Multicast addresses:
Vlan MAC Address Ports
---- ----------------- -----
8 01:00:5e:02:02:03 te1/0/4
Multicast address table for VLANs in IPv4-GROUP bridging mode:
Vlan MAC Address Type Ports
---- ----------------- -------------- -----
1 224.0.0.251 Dynamic te1/0/2
Forbidden ports for Multicast addresses:
Vlan MAC Address Ports
---- ----------------- -----
1 232.5.6.5
1 233.22.2.6
Multicast address table for VLANs in IPv4-SRC-GROUP bridging mode:
Vlan Group Address Source address Type Ports
---- --------------- --------------- -------- -----
1 224.2.2.251 11.2.2.3 Dynamic te1/0/1
Forbidden ports for Multicast addresses:
Vlan Group Address Source Address Ports
---- --------------- --------------- -------
8 239.2.2.2 * te1/0/4
8 239.2.2.2 1.1.1.11 te1/0/4
Multicast address table for VLANs in IPv6-GROUP bridging mode:
VLAN IP/MAC Address Type Ports
---- ----------------- --------- ---------------------
8 ff02::4:4:4 Static te1/0/1-2, te1/0/3, Po1
Forbidden ports for Multicast addresses:
```

```
VLAN IP/MAC Address Ports
---- ----------------- -----------
8 ff02::4:4:4 te1/0/4
Multicast address table for VLANs in IPv6-SRC-GROUP bridging mode:
Vlan Group Address Source address Type Ports
---- --------------- --------------- -------- -----------------
8 ff02::4:4:4 * Static te1/0/1-2,te1/0/3,Po1
8 ff02::4:4:4 fe80::200:7ff: Static fe00:200
Forbidden ports for Multicast addresses:
Vlan Group Address Source address Ports
---- --------------- --------------- ----------
8 ff02::4:4:4 * te1/0/4 8 ff02::4:4:4 fe80::200:7ff:f te1/0/4 e00:200
```

5.30. show bridge multicast address-table static

To display the statically-configured Multicast addresses, use the `show bridge multicast address-table static` Privileged EXEC mode command.

Syntax

- show bridge multicast address-table static [vlan vlan-id] [all]
- show bridge multicast address-table static [vlan vlan-id] [address mac-multicast-address] [mac| ip]
- show bridge multicast address-table static [vlan vlan-id] [address ipv4-multicast-address] [source ipv4-source-address]
- show bridge multicast address-table static [vlan vlan-id] [address ipv6-multicast-address] [source ipv6-source-address]

Parameters

- vlan vlan-id - (Optional) Specifies the VLAN ID.
- address - (Optional) Specifies the Multicast address. The possible values are:
  - mac-multicast-address - (Optional) Specifies the MAC Multicast address.
  - ipv4-multicast-address - (Optional) Specifies the IPv4 Multicast address.
  - ipv6-multicast-address - (Optional) Specifies the IPv6 Multicast address.
- source - (Optional) Specifies the source address. The possible values are:
  - ipv4-address - (Optional) Specifies the source IPv4 address.
  - ipv6-address - (Optional) Specifies the source IPv6 address.

Default Configuration

When all/mac/ip is not specified, all entries (MAC and IP) will be displayed.

Command Mode

Privileged EXEC mode

User Guidelines

A MAC address can be displayed in IP format only if it is within the range 0100.5e00.0000–-0100.5e7f.ffff.

Example

The following example displays the statically-configured Multicast addresses.

```
switchxxxxxx# show bridge multicast address-table static
MAC-GROUP table
Vlan MAC Address Ports
```

```
---- -------------- --------
1 0100.9923.8787 te1/0/1, te1/0/2
Forbidden ports for multicast addresses:
Vlan MAC Address Ports
---- -------------- --------

IPv4-GROUP Table
Vlan IP Address Ports
---- ---------- -------
1 231.2.2.3 te1/0/1, te1/0/2
19 231.2. te1/0/2-3
Forbidden ports for multicast addresses:
Vlan IP Address Ports
---- ---------- --------
1 231.2. te1/0/4
19 231.2. te1/0/3

IPv4-SRC-GROUP Table:
Vlan Group Address Source address
---- -------------- ---------------
Forbidden ports for multicast addresses:
Vlan Group Address Source address
---- -------------- ---------------

IPv6-GROUP Table
Vlan IP Address Ports
---- ---------- ---------
191 FF12::8 te1/0/1-4
Forbidden ports for multicast addresses:
Vlan IP Address Ports
---- ---------- ---------
11 FF12::3 te1/0/4
191 FF12::8 te1/0/4
IPv6-SRC-GROUP Table:
Vlan  Group Address     Source address
----  ---------------   ---------------
192   FF12::8     FE80::201:C9A9:FE40:
8988
Forbidden ports for multicast addresses:  Ports -----te1/0/1-4
Vlan  Group Address     Source address
----  ---------------   ---------------
192   FF12::3     FE80::201:C9A9:FE40
:8988 Ports -----te1/0/4
```

5.31. show bridge multicast filtering

To display the Multicast filtering configuration, use the `show bridge multicast filtering` Privileged EXEC mode command.

Syntax

- show bridge multicast filtering vlan-id

Parameters

- vlan-id - Specifies the VLAN ID. (Range: Valid VLAN)

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example displays the Multicast configuration for VLAN 1.

```
switchxxxxxx# show bridge multicast filtering 1
Filtering: Enabled
VLAN: 1
Forward-All
Port Static Status
---- --------- ------
te1/0/1 Forbidden Filter
te1/0/2 Forward Forward(s)
te1/0/3 - Forward(d)
```

5.32. show bridge multicast unregistered

To display the unregistered Multicast filtering configuration, use the `show bridge multicast unregistered` Privileged EXEC mode command.

Syntax

- show bridge multicast unregistered [interface-id]

Parameters

- interface-id - (Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

Display for all interfaces.

Command Mode

Privileged EXEC mode

Example

The following example displays the unregistered Multicast configuration.

```
switchxxxxxx# show bridge multicast unregistered
Port Unregistered
------ -------------
te1/0/1 Forward
te1/0/2 Filter
te1/0/3 Filter
```

5.33. show ports security

To display the port-lock status, use the `show ports security` Privileged EXEC mode command.

Syntax

- show ports security [interface-id | detailed]

Parameters

- interface-id - (Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- detailed - (Optional) Displays information for non-present ports in addition to present ports.

Default Configuration

Display for all interfaces. If detailed is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays the port-lock status of all ports.

```
switchxxxxxx# show ports security
Port Status Learning Action Maximum Trap Frequency
------- -------- -------- ------ ------- ------- --------
te1/0/1 Enabled Max- Discard 3 Enabled 100 Addresses
te1/0/2 Disabled Max- - 28 - Addresses
te1/0/3 Enabled Lock Discard 8 Disabled -
```

The following table describes the fields shown above.

Field	Description
Port	The port number.
Status	The port security status. The possible values are: Enabled or Disabled.
Action	The action taken on violation.
Maximum	The maximum number of addresses that can be associated on this port in the Max-Addresses mode.
Trap	The status of SNMP traps. The possible values are: Enable or Disable.
Frequency	The minimum time interval between consecutive traps.

5.34. show ports security addresses

To display the current dynamic addresses in locked ports, use the `show ports security addresses` Privileged EXEC mode command.

Syntax

- show ports security addresses [interface-id | detailed]

Parameters

- interface-id - (Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- detailed - (Optional) Displays information for non-present ports in addition to present ports.

Default Configuration

Display for all interfaces. If detailed is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays dynamic addresses in all currently locked port:

```
switchxxxxxx# show ports security addresses
Port Status Learning Current Maximum
------ ------ -------- ------- -------
te1/0/1 Disabled Lock 0 10
te1/0/2 Disabled Lock 0 1
te1/0/3 Disabled Lock 0 1
te1/0/4 Disabled Lock 0 1
```

5.35. bridge multicast reserved-address

To define the action on Multicast reserved-address packets, use the `bridge multicast reserved-address` Global Configuration mode command. To revert to default, use the no form of this command.

Syntax

- bridge multicast reserved-address mac-multicast-address [ethernet-v2 ethtype | llc sap | llc-snap pid] {discard | bridge}
- no bridge multicast reserved-address mac-multicast-address [ethernet-v2 ethtype | llc sap | llc-snap pid]

Parameters

- mac-multicast-address - MAC Multicast address in the reserved MAC addresses range. (Range: 01-80-C2-00-00-00, 01-80-C2-00-00-02–01-80-C2-00-00-2F)
- ethernet-v2 ethtype - (Optional) Specifies that the packet type is Ethernet v2 and the Ethernet type field (16 bits in hexadecimal format). (Range: 0x0600–0xFFFF)
- llc sap - (Optional) Specifies that the packet type is LLC and the DSAP-SSAP field (16 bits in hexadecimal format). (Range: 0xFFFF)
- llc-snap pid - (Optional) Specifies that the packet type is LLC-SNAP and the PID field (40 bits in hexadecimal format). (Range: 0x0000000000 - 0xFFFFFFFFFF)
- discard - Specifies discarding the packets.
- bridge - Specifies bridging (forwarding) the packets

Default Configuration

- If the user-supplied MAC Multicast address, ethertype and encapsulation (LLC) specifies a protocol supported on the device (called Peer), the default action (discard or bridge) is determined by the protocol.
- If not, the default action is as follows:
  - For MAC addresses in the range 01-80-C2-00-00-00, 01-80-C2-00-00-02– 01-80-C2-00-00-0F, the default is discard.
  - For MAC addresses in the range 00-80-C2-00-00-10– 01-80-C2-00-00-2F, the default is bridge.

Command Mode

Global Configuration mode

User Guidelines

If the packet/service type (ethertype/encapsulation) is not specified, the configuration is relevant to all the packets with the configured MAC address.

Specific configurations (that contain service type) have precedence over less specific configurations (contain only MAC address).

The packets that are bridged are subject to security ACLs.

The actions define by this command has precedence over forwarding rules defined by applications/protocols (STP, LLDP etc.) supported on the device.

Example

```
switchxxxxxx(config)# bridge multicast reserved-address 00:3f:bd:45:5a:b1
```

5.36. show bridge multicast reserved-addresses

To display the Multicast reserved-address rules, use the `show bridge multicast reserved-addresses` Privileged EXEC mode command.

Syntax

- show bridge multicast reserved-addresses

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx # show bridge multicast reserved-addresses
MAC Address Frame Type Protocol Action
------------------ ----------- -------------- ------------
01-80-C2-00-00-00 LLC-SNAP 00-00-0C-01-29 Bridge
```

6. Auto-Update and Auto-Config

6.1. boot host auto-config

Use the `boot host auto-config` Global Configuration mode command to enable auto configuration via DHCP. Use the no form of this command to disable DHCP auto configuration.

Syntax

- boot host auto-config [tftp | scp | auto [extension]]
- no boot host auto-config

Parameters

- tftp - Only the TFTP protocol is used by auto-configuration.
- scp - Only the SCP protocol is used by auto-configuration.
- auto - (Default) Auto-configuration uses the TFTP or SCP protocol depending on the configuration file's extension. If this option is selected, the extension parameter may be specified or, if not, the default extension is used.
- extension - The SCP file extension. When no value is specified, 'scp' is used. (Range: 1-16 characters)

Default Configuration

Auto configuration via DHCP is disabled.

Command Mode

Global Configuration mode

User Guidelines

The TFTP or SCP protocol is used to download/upload a configuration file.

Examples

Example 1. The following example specifies the auto mode and specifies "scon" as the SCP extension:

```
switchxxxxxx(config)# boot host auto-config auto scon
```

Example 2. The following example specifies the auto mode and does not provide an SCP extension.

```
In this case "scp" is used.
switchxxxxxx(config)# boot host auto-config auto
```

Example 3. The following example specifies that only the SCP protocol will be used:

```
switchxxxxxx(config)# boot host auto-config scp
```

6.2. boot host auto-update

Use the `boot host auto-update` Global Configuration mode command to enable the support of auto update via DHCP. Use the no form of this command to disable DHCP auto configuration.

Syntax

- boot host auto-update [tftp | scp | auto [extension]]
- no boot host auto-update

Parameters

- tftp - Only the TFTP protocol is used by auto-update.
- scp - Only the SCP protocol is used by auto-update.
- auto (Default) - Auto-configuration uses the TFTP or SCP protocol depending on the Indirect image file's extension. If this option is selected, the extension parameter may be specified or, if not, the default extension is used.
- extension - The SCP file extension. When no value is specified, 'scp' is used. (Range: 1-16 characters)

Default Configuration

Auto update via DHCP is disabled.

Command Mode

Global Configuration mode

User Guidelines

The TFTP or SCP protocol is used to download/upload an image file.

Examples

Example 1 - The following example specifies the auto mode and specifies "scon" as the SCP extension:

```
switchxxxxxx(config)# boot host auto-update auto scon
```

Example 2 - The following example specifies the auto mode and does not provide an SCP extension. In this case "scp" is used.

```
switchxxxxxx(config)# boot host auto-update auto
```

Example 3 - The following example specifies that only the SCP protocol will be used:

```
switchxxxxxx(config)# boot host auto-update scp
```

6.3. show boot

Use the `show boot` Privilege EXEC mode command to show the status of the IP DHCP Auto Config process.

Syntax

- show boot

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Examples

```
switchxxxxxx# show boot
Auto Config
------------
```

```
Config Download via DHCP: enabled
Download Protocol: auto
SCP protocol will be used for files with extension: scp
Configuration file auto-save: enabled
Auto Config State: Finished successfully
Server IP address: 1.2.20.2
Configuration filename: /config/configfile1.cfg
 Auto Update
 ----------
Image Download via DHCP: enabled
switchxxxxxx# show boot
Auto Config
------------
Config Download via DHCP: enabled
Download Protocol: scp
Configuration file auto-save: enabled
Auto Config State: Opening <hostname>-config file
 Auto Update
 -----------
Image Download via DHCP: enabled
switchxxxxxx# show boot
Auto Config
------------
Config Download via DHCP: enabled
"Download Protocol: scp
Configuration file auto-save: enabled
Auto Config State: Downloading configuration file
 Auto Update
 -----------
Image Download via DHCP: enabled
switchxxxxxx# show boot
Auto Config
------------
Config Download via DHCP: enabled
Download Protocol: tftp
Configuration file auto-save: enabled
Auto Config State: Searching device hostname in indirect file
 Auto Update
 -----------
Image Download via DHCP: enabled
switchxxxxxx# show boot
Auto Config
------------
Config Download via DHCP: enabled
Download Protocol: tftp
Configuration file auto-save: enabled
 Auto Update
 -----------
Image Download via DHCP: enabled
Auto Update State: Downloaded indirect image file
Indirect Image filename: /image/indirectimage.txt
```

6.4. ip dhcp tftp-server ip address

Use the `ip dhcp tftp-server ip address` Global Configuration mode command to set the backup server’s IP address. This address server as the default address used by a switch

when it has not been received from the DHCP server. Use the no form of the command to return to default.

Syntax

- ip dhcp tftp-server ip address ip-addr
- no ip dhcp tftp-server ip address

Parameters

- ip-addr - IPv4 Address, or IPv6 Address or DNS name of TFTP or SCP server.

Default Configuration

No IP address

Command Mode

Global Configuration mode

User Guidelines

The backup server can be a TFTP server or a SCP server.

Examples

Example 1. The example specifies the IPv4 address of TFTP server:

```
switchxxxxxx(config)# ip dhcp tftp-server ip address 10.5.234.232
```

Example 2. The example specifies the IPv6 address of TFTP server:

```
switchxxxxxx(config)# ip dhcp tftp-server ip address 3000:1::12
```

Example 3. The example specifies the IPv6 address of TFTP server:

```
switchxxxxxx(config)# ip dhcp tftp-server ip address tftp-server.company.com
```

6.5. ip dhcp tftp-server file

Use the `ip dhcp tftp-server file` Global Configuration mode command to set the full file name of the configuration file to be downloaded from the backup server when it has not been received from the DHCP server. Use the no form of this command to remove the name.

Syntax

- ip dhcp tftp-server file file-path
- no ip dhcp tftp-server file

Parameters

- file-path - Full file path and name of the configuration file on the server.

Default Configuration

No file name

Command Mode

Global Configuration mode

User Guidelines

The backup server can be a TFTP server or an SCP server.

Examples

```
switchxxxxxx(config)# ip dhcp tftp-server file conf/conf-file
```

6.6. ip dhcp tftp-server image file

Use the `ip dhcp tftp-server image file` Global Configuration mode command to set the indirect file name of the image file to be downloaded from the backup server when it has not been received from the DHCP server. Use the no form of this command to remove the file name.

Syntax

- ip dhcp tftp-server image file file-path
- no ip dhcp tftp-server image file

Parameters

- file-path - Full indirect file path and name of the configuration file on the server.

Default Configuration

No file name

Command Mode

Global Configuration mode

User Guidelines

The backup server can be a TFTP server or a SCP server.

Examples

```
switchxxxxxx(config)# ip dhcp tftp-server image file imag/imag-file
```

6.7. show ip dhcp tftp-server

Use the `show ip dhcp tftp-server` EXEC mode command to display information about the backup server.

Syntax

- show ip dhcp tftp-server

Parameters

N/A

Default Configuration

N/A

Command Mode

User EXEC mode

User Guidelines

The backup server can be a TFTP server or a SCP server.

Example

```
show ip dhcp tftp-server server address
active      1.1.1.1 from sname manual     2.2.2.2
```

```
file path on server active    conf/conf-file from option 67 manual
      conf/conf-file1
```

7. Clock Commands

7.1. clock dhcp timezone

To specify that the timezone and the Summer Time (Daylight Saving Time) of the system can be taken from the DHCP Timezone option, use the `clock dhcp timezone` command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- clock dhcp timezone
- no clock dhcp timezone

Parameters

N/A

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

The TimeZone taken from the DHCP server has precedence over the static TimeZone.

The Summer Time taken from the DHCP server has precedence over static SummerTime.

The TimeZone and SummerTime remain effective after the IP address lease time has expired.

The TimeZone and SummerTime that are taken from the DHCP server are cleared after reboot.

The no form of the command clears the dynamic Time Zone and Summer Time from the DHCP server are cleared.

In case of multiple DHCP-enabled interfaces, the following precedence is applied:

- information received from DHCPv6 precedes information received from DHCPv4
- information received from DHCP client running on lower interface precedes information received from DHCP client running on higher interface

Disabling the DHCP client from where the DHCP-TimeZone option was taken, clears the dynamic Time Zone and Summer Time configuration.

Example

```
switchxxxxxx(config)# clock dhcp timezone
```

7.2. clock set

To set the system clock manually, use the `clock set` command in Privileged EXEC mode.

Syntax

- clock set hh:mm:ss {[day month] | [month day]} year

Parameters

- *hh:mm:ss* - Specifies the current time in hours (military format), minutes, and seconds. (Range: hh: 0-23, mm: 0-59, ss: 0-59)

- *day* - Specifies the current day of the month. (Range: 1-31)
- month - Specifies the current month using the first three letters of the month name. (Range: Jan–Dec)
- year - Specifies the current year. (Range: 2000–2037)

Default Configuration

The time of the image creation.

Command Mode

Privileged EXEC mode

User Guidelines

After boot the system clock is set to the time of the image creation.

Example

The following example sets the system time to 13:32:00 on March 7th, 2005.

```
switchxxxxxx# clock set 13:32:00 7 Mar 2005
```

7.3. clock source

To configure an external time source for the system clock, use the `clock source` command in Global Configuration mode. To disable the external time source, use the no form of this command.

Syntax

- clock source sntp
- no clock source sntp

Parameters

- sntp - (Optional) Specifies that an SNTP server is the external clock source.

Default Configuration

There is no external clock source.

Command Mode

Global Configuration mode

User Guidelines

After boot the system clock is set to the time of the image creation.

If no parameter is specified, SNTP will be configured as the time source.

Example

The following example configures an SNTP server as an external time source for the system clock.

```
switchxxxxxx(config)# clock source sntp
switchxxxxxx(config)# exit
switchxxxxxx# show clock
*10:46:48 UTC May 28 2013
Time source is sntp
```

7.4. clock summer-time

To configure the system to automatically switch to summer time (Daylight Saving Time), use the `clock summer-time` command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- clock summer-time zone recurring {usa | eu | {week day month hh:mm week day month hh:mm}} [offset]
- clock summer-time zone date day month year hh:mm date month year hh:mm [offset]
- clock summer-time zone date month day year hh:mm month day year hh:mm [offset]
- no clock summer-time

Parameters

- zone - The acronym of the time zone to be displayed when summer time is in effect. (Range: up to 4 characters)
- recurring - Indicates that summer time starts and ends on the corresponding specified days every year.
- date - Indicates that summer time starts on the first date listed in the command and ends on the second date in the command.
- usa - The summer time rules are the United States rules.
- eu - The summer time rules are the European Union rules.
- week - Week of the month. Can be 1–5, first to last.
- day - Day of the week (first three characters by name, such as Sun).
- date - Date of the month. (Range: 1–31)
- month - Month (first three characters by name, such as Feb).
- year - year (no abbreviation). (Range: 2000–2097)
- hh:mm - Time (military format) in hours and minutes. (Range: hh:mmhh: 0-23, mm: 0-59)
- offset - (Optional) Number of minutes to add during summer time (default is 60). (Range: 1440)

Default Configuration

Summer time is disabled.

Command Mode

Global Configuration mode

User Guidelines

In both the date and recurring forms of the command, the first part of the 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 chronologically after the ending month, the system assumes that you are in the southern hemisphere.

USA rules for Daylight Saving Time:

- From 2007:
- Start: Second Sunday in March
- End: First Sunday in November
- Time: 2 AM local time
- Before 2007:
- Start: First Sunday in April

- End: Last Sunday in October
- Time: 2 AM local time

EU rules for Daylight Saving Time:

- Start: Last Sunday in March
- End: Last Sunday in October
- Time: 1.00 am (01:00) Greenwich Mean Time (GMT)

Example

```
switchxxxxxx(config)# clock summer-time abc date apr 1 2010 09:00 aug 2 2010
09:00
```

7.5. clock timezone

To set the time zone for display purposes, use the `clock timezone` command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- clock timezone zone hours-offset [minutes-offset]
- no clock timezone

Parameters

- zone - The acronym of the time zone. (Range: Up to 4 characters)
- hours-offset - Hours difference from UTC. (Range: (-12)–(+13))
- minutes-offset - (Optional) Minutes difference from UTC. (Range: 0–59)

Default Configuration

Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT), which is the same:

- Offsets are 0.
- Acronym is empty.

Command Mode

Global Configuration mode

User Guidelines

The system internally keeps time in UTC, so this command is used only for display purposes and when the time is manually set.

Example

```
switchxxxxxx(config)# clock timezone abc +2 minutes 32
```

7.6. sntp anycast client enable

To enable the SNTP Anycast client, use the `sntp anycast client enable` command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- sntp anycast client enable [both | ipv4 | ipv6]

Parameters

- both - (Optional) Specifies the IPv4 and IPv6 SNTP Anycast clients are enabled. If the parameter is not defined it is the default value.

- ipv4 - (Optional) Specifies the IPv4 SNTP Anycast clients are enabled.
- ipv6 - (Optional) Specifies the IPv6 SNTP Anycast clients are enabled.

Default Configuration

The SNTP anycast client is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use this command to enable the SNTP Anycast client.

Example

The following example enables SNTP Anycast clients.

```
switchxxxxxx(config)# sntp anycast client enable
```

7.7. sntp authenticate

To enable authentication for received SNTP traffic from servers, use the `sntp authenticate` command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- sntp authenticate
- no sntp authenticate

Parameters

N/A

Default Configuration

Authentication is disabled.

Command Mode

Global Configuration mode

Examples

The following example enables authentication for received SNTP traffic and sets the key and encryption key.

```
switchxxxxxx(config)# sntp authenticate
switchxxxxxx(config)# sntp authentication-key 8 md5 ClkKey
switchxxxxxx(config)# sntp trusted-key 8
```

7.8. sntp authentication-key

To define an authentication key for Simple Network Time Protocol (SNTP), use the `sntp authentication-key` command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- sntp authentication-key key-number md5 key-value
- no sntp authentication-key key-number

Parameters

- key-number - Specifies the key number. (Range: 1–4294967295)
- key-value - Specifies the key value. (Length: 1–8 characters)

Default Configuration

No authentication key is defined.

Command Mode

Global Configuration mode

Examples

The following example defines the authentication key for SNTP.

```
switchxxxxxx(config)# sntp authentication-key 8 md5 ClkKey
switchxxxxxx(config)# sntp authentication-key 8 md5 ClkKey
switchxxxxxx(config)# sntp trusted-key 8
switchxxxxxx(config)# sntp authenticate
```

7.9. sntp broadcast client enable

To enable SNTP Broadcast clients, use the `sntp broadcast client enable` command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- sntp broadcast client enable [both | ipv4 | ipv6]
- no sntp broadcast client enable

Parameters

- both - (Optional) Specifies the IPv4 and IPv6 SNTP Broadcast clients are enabled. If the parameter is not defined it is the default value.
- ipv4 - (Optional) Specifies the IPv4 SNTP Broadcast clients are enabled.
- ipv6 - (Optional) Specifies the IPv6 SNTP Broadcast clients are enabled.

Default Configuration

The SNTP Broadcast client is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the `sntp broadcast client enable` Interface Configuration mode command to enable the SNTP Broadcast client on a specific interface.

After entering this command, you must enter the `clock source` command with the sntp keyword for the command to be run. If this command is not run, the switch will not synchronize with Broadcast servers.

Example

The following example enables SNTP Broadcast clients.

```
switchxxxxxx(config)# sntp broadcast client enable
```

7.10. sntp client enable

To enable the SNTP Broadcast and Anycast client, use the `sntp client enable` command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- sntp client enable interface-id
- no sntp client enable interface-id

Parameters

- interface-id - Specifies an interface ID, which can be one of the following types:
  - Ethernet port,
  - Port-channel or
  - VLAN.

Default Configuration

The SNTP client is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the `sntp client enable` command to enable SNTP Broadcast and Anycast clients.

Example

The following example enables the SNTP Broadcast and Anycast clients on VLAN 100:

```
switchxxxxxx(config)# sntp client enable vlan 100
```

7.11. sntp client enable (interface)

To enable the SNTP Broadcast and Anycast client on an interface, use the `sntp client enable` command in Interface Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

sntp client enable no sntp client enable

Parameters

N/A

Default Configuration

The SNTP client is disabled on an interface.

Command Mode

Interface Configuration mode

User Guidelines

This command enables the SNTP Broadcast and Anycast client on an interface. Use the no form of this command to disable the SNTP client.

Example

The following example enables the SNTP broadcast and anycast client on an interface.

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# sntp client enable
switchxxxxxx(config-if)# exit
```

7.12. sntp server

To configure the device to use the SNTP to request and accept Network Time Protocol (NTP) traffic from a specified server (meaning to accept system time from an SNTP server), use the `sntp server` command in Global Configuration mode. To remove a server from the list of SNTP servers, use the no form of this command.

Syntax

- sntp server {ip-address | hostname} [poll] [key keyid]
- no sntp server [ip-address | hostname]

Parameters

- ip-address - Specifies the server IP address. This can be an IPv4, IPv6 or IPv6 address.
- hostname - Specifies the server hostname. Only translation to IPv4 addresses is supported. (Length: 1–158 characters. Maximum label length for each part of the hostname: 63 characters)
- poll - (Optional) Enables polling.
- key keyid - (Optional) Specifies the Authentication key to use when sending packets to this peer. (Range:1–4294967295)

Default Configuration

No servers are defined.

Command Mode

Global Configuration mode

User Guidelines

Use the sntp server {ip-address | hostname} [poll] [key keyid] command to define a SNTP server. The switch supports up to 8 SNTP servers.

Use the no sntp server ip-address | hostname command to remove one SNTP server.

Use the no sntp server to remove all SNTP servers.

Example

The following example configures the device to accept SNTP traffic from the server on 192.1.1.1 with polling.

```
switchxxxxxx(config)# sntp server 192.1.1.1 poll
```

7.13. sntp source-interface

To specify the source interface whose IPv4 address will be used as the source IPv4 address for communication with IPv4 SNTP servers, use the `sntp source-interface` command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- sntp source-interface interface-id
- no sntp source-interface

Parameters

- interface-id - Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the interface IP address belonging to next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface, the minimal IPv4 address defined on the interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 SNTP server.

OOB cannot be defined as a source interface.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# sntp source-interface vlan 10
```

7.14. sntp source-interface-ipv6

To specify the source interface whose IPv6 address will be used ad the Source IPv6 address for communication with IPv6 SNTP servers, use the `sntp source-interface-ipv6` command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- sntp source-interface-ipv6 interface-id
- no sntp source-interface-ipv6

Parameters

- interface-id - Specifies the source interface.

Default Configuration

The IPv6 source address is the IPv6 address defined of the outgoing interface and selected in accordance with RFC6724.

Command Mode

Global Configuration mode

User Guidelines

The outgoing interface is selected based on the SNTP server's IP address. If the source interface is the outgoing interface, the IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

If the source interface is not the outgoing interface, the minimal IPv4 address defined on the interface and with the scope of the destination IPv6 address is applied.

If there is no available IPv6 source address, a SYSLOG message is issued when attempting to communicate with an IPv6 SNTP server.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# sntp source-interface-ipv6 vlan 10
```

7.15. sntp trusted-key

To define the trusted key, use the `sntp trusted-key` command in Global

Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- sntp trusted-key key-number
- no sntp trusted-key key-number

Parameters

- key-number - Specifies the key number of the authentication key to be trusted. (Range: 1–4294967295).

Default Configuration

No keys are trusted.

Command Mode

Global Configuration mode

User Guidelines

The trusted key is used for authentication of all servers not having personal keys assigned by the `sntp server` command.

Examples

The following example authenticates key 8.

```
switchxxxxxx(config)# sntp trusted-key 8
switchxxxxxx(config)# sntp authentication-key 8 md5 ClkKey
switchxxxxxx(config)# sntp trusted-key 8
switchxxxxxx(config)# sntp authenticate
```

7.16. sntp unicast client enable

To enable the device to use Simple Network Time Protocol (SNTP) Unicast clients, use the `sntp unicast client enable` command in Global Configuration mode. To disable the SNTP Unicast clients, use the no form of this command.

Syntax

- sntp unicast client enable
- no sntp unicast client enable

Parameters

N/A

Default Configuration

The SNTP unicast clients are disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the `sntp server` Global Configuration mode command to define SNTP servers.

Example

The following example enables the device to use SNTP Unicast clients.

```
switchxxxxxx(config)# sntp unicast client enable
```

7.17. sntp unicast client poll

To enable polling for the SNTP Unicast clients, use the `sntp unicast client poll` command in Global Configuration mode. To disable the polling, use the no form of this command.

Syntax

- sntp unicast client poll
- no sntp unicast client poll

Parameters

N/A

Default Configuration

Polling is disabled.

Command Mode

Global Configuration mode

User Guidelines

The polling interval is 1024 seconds.

Example

The following example enables polling for SNTP unicast clients.

```
switchxxxxxx(config)# sntp unicast client poll
```

7.18. show clock

To display the time and date from the system clock, use the `show clock` command in User EXEC mode.

Syntax

- show clock [detail]

Parameters

- detail - (Optional) Displays the time zone and summer time configuration.

Command Mode

User EXEC mode

User Guidelines

Before the time, there is displayed either a star (*), period (.), or blank:

- star (*) - The clock is invalid.
- period (.) - The clock was set manually.
- blank - The clock was set by SNTP.

Examples

Example 1 - The following example displays the system time and date.

```
switchxxxxxx# show clock
 15:29:03 PDT(UTC-7) Jun 17 2002
Time source is SNTP
```

Example 2 - The following example displays the system time and date along with the time zone and summer time configuration.

```
switchxxxxxx# show clock detail
 15:22:55 SUN Apr 23 2012
Time source is sntp
Time zone (DHCPv4 on VLAN1):
Acronym is RAIN
Offset is UTC+2
Time zone (Static):
Offset is UTC+0
Summertime (DHCPv4 on VLAN1):
Acronym is SUN
Recurring every year.
Begins at first Sunday of Apr at 02:00.
Ends at first Tuesday of Sep at 02:00.
Offset is 60 minutes.
Summertime (Static):
Acronym is GMT
Recurring every year.
Begins at first Sunday of Mar at 10:00.
Ends at first Sunday of Sep at 10:00.
Offset is 60 minutes.
DHCP timezone: Enabled
```

7.19. show sntp configuration

To display the SNTP configuration on the device, use the `show sntp configuration` command in Privileged EXEC mode.

Syntax

- show sntp configuration

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Examples

The following example displays the device’s current SNTP configuration.

```
switchxxxxxx# show sntp configuration
SNTP port : 123
Polling interval: 1024 seconds
MD5 Authentication Keys
-----------------------------------
John123
Alice456
-----------------------------------
Authentication is not required for synchronization.
No trusted keys
Unicast Clients: enabled
Unicast Clients Polling: enabled
Server: 1.1.1.121
 Polling: disabled
 Encryption Key: disabled
Server: 3001:1:1::1
 Polling: enabled
 Encryption Key: disabled
Server: dns_server1.comapany.com
 Polling: enabled
 Encryption Key: disabled
Server: dns_server2.comapany.com
 Polling: enabled
 Encryption Key: disabled
Broadcast Clients: enabled for IPv4 and IPv6
Anycast Clients: disabled
No Broadcast Interfaces
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
```

7.20. show sntp status

To display the SNTP servers status, use the `show sntp status` command in Privileged EXEC mode.

Syntax

- show sntp status

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays the SNTP servers status:

```
switchxxxxxx# show sntp status
Clock is synchronized, stratum 4, reference is 176.1.1.8, unicast
Reference time is afe2525e.70597b34 (00:10:22.438 PDT Jul 5 1993) Unicast
servers:
Server: 176.1.1.8
 Source: DHCPv4 on VLAN 1
 Status: Up
 Last response: 19:58:22.289 PDT Feb 19 2005
 Stratum Level: 1
 Offset: 7.33mSec
 Delay: 117.79mSec
Server: dns_server.comapany.com
 Source: static
 Status: Unknown
 Last response: 12:17.17.987 PDT Feb 19 2005
 Stratum Level: 1
 Offset: 8.98mSec
 Delay: 189.19mSec
Server: 3001:1:1::1
 Source: DHCPv6 on VLAN 2
 Status: Unknown Last response:
 Offset: mSec
 Delay: mSec
Server: dns1.company.com
 Source: DHCPv6 on VLAN 20
 Status: Unknown Last response:
 Offset: mSec
 Delay: mSec
Anycast servers:
Server: 176.1.11.8
 Interface: VLAN 112
 Status: Up
 Last response: 9:53:21.789 PDT Feb 19 2005
 Stratum Level: 10 Offset: 9.98mSec
 Delay: 289.19mSec Broadcast servers: Server: 3001:1::12
 Interface: VLAN 101
 Last response: 9:53:21.789 PDT Feb 19 2005
 Stratum Level: 255
```

8. DHCP Relay Commands

8.1. ip dhcp relay enable (Global)

Use the `ip dhcp relay enable` Global Configuration mode command to enable the DHCP relay feature on the device. Use the no form of this command to disable the DHCP relay feature.

Syntax

- ip dhcp relay enable
- no ip dhcp relay enable

Parameters

N/A

Default Configuration

DHCP relay feature is disabled.

Command Mode

Global Configuration mode

Example

The following example enables the DHCP relay feature on the device.

```
switchxxxxxx(config)# ip dhcp relay enable
```

8.2. ip dhcp relay enable (Interface)

Use the `ip dhcp relay enable` Interface Configuration mode command to enable the DHCP relay feature on an interface. Use the no form of this command to disable the DHCP relay agent feature on an interface.

Syntax

- ip dhcp relay enable
- no ip dhcp relay enable

Parameters

N/A

Default Configuration

Disabled

Command Mode

Interface Configuration mode

User Guidelines

The operational status of DHCP Relay on an interface is active if one of the following conditions exist:

- DHCP Relay is globally enabled, and there is an IP address defined on the interface.
-
- Or:
-

- DHCP Relay is globally enabled, there is no IP address defined on the interface, the interface is a VLAN, and option 82 is enabled.

Example

The following example enables DHCP Relay on VLAN 21.

```
switchxxxxxx(config)# interface vlan 21
switchxxxxxx(config-if)# ip dhcp relay enable
```

8.3. ip dhcp relay address (Global)

Use the `ip dhcp relay address` Global Configuration mode command to define the DHCP servers available for the DHCP relay. Use the no form of this command to remove the server from the list.

Syntax

- ip dhcp relay address ip-address
- no ip dhcp relay address [ip-address]

Parameters

- ip-address - Specifies the DHCP server IP address. Up to 8 servers can be defined.

Default Configuration

No server is defined.

Command Mode

Global Configuration mode

User Guidelines

Use the `ip dhcp relay address` command to define a global DHCP Server IP address. To define a few DHCP Servers, use the command a few times.

To remove a DHCP Server, use the no form of the command with the ip-address argument.

The no form of the command without the ip-address argument deletes all global defined DHCP servers.

Example

The following example defines the DHCP server on the device.

```
switchxxxxxx(config)# ip dhcp relay address 176.16.1.1
```

8.4. ip dhcp relay address (Interface)

Use the `ip dhcp relay address` Interface Configuration (VLAN, Ethernet, Port-channel) command to define the DHCP servers available by the DHCP relay for DHCP clients connected to the interface. Use the no form of this command to remove the server from the list.

Syntax

- ip dhcp relay address ip-address
- no ip dhcp relay address [ip-address]

Parameters

- ip-address - Specifies the DHCP server IP address. Up to 8 servers can be defined.

Default Configuration

No server is defined.

Command Mode

Interface Configuration mode

User Guidelines

Use the `ip dhcp relay address` command to define a DHCP Server IP address per the interface. To define multiple DHCP Servers, use the command multiple times.

To remove a DHCP server, use the no form of the command with the ip-address argument.

The no form of the command without the ip-address argument deletes all DHCP servers.

Example

The following example defines the DHCP server on the device.

```
switchxxxxxx(config)# interface vlan 21
switchxxxxxx(config-if)# ip dhcp relay address 176.16.1.1
```

8.5. show ip dhcp relay

Use the `show ip dhcp relay` EXEC mode command to display the DHCP relay information.

Syntax

- show ip dhcp relay

Command Mode

User EXEC mode

Examples

Example 1. Option 82 is not supported:

```
switchxxxxxx# show ip dhcp relay
DHCP relay is globally enabled
Option 82 is Disabled
Maximum number of supported VLANs without IP Address is 256 Number of DHCP
Relays enabled on VLANs without IP Address is 0
DHCP relay is not configured on any port.
DHCP relay is not configured on any vlan.
No servers configured
```

Example 2. Option 82 is supported (disabled):

```
switchxxxxxx# show ip dhcp relay
DHCP relay is globally disabled
Option 82 is disabled
Maximum number of supported VLANs without IP Address: 0
Number of DHCP Relays enabled on VLANs without IP Address: 4
DHCP relay is enabled on Ports: te1/0/1,po1-2
 Active:
 Inactive: te1/0/1, po1-4
DHCP relay is enabled on VLANs: 1, 2, 4, 5
 Active:
 Inactive: 1, 2, 4, 5
```

```
Global Servers: 1.1.1.1 , 2.2.2.2
```

Example 3. Option 82 is supported (enabled):

```
switchxxxxxx# show ip dhcp relay
DHCP relay is globally enabled
Option 82 is enabled
Maximum number of supported VLANs without IP Address is 4
Number of DHCP Relays enabled on VLANs without IP Address: 2
DHCP relay is enabled on Ports: te1/0/1,po1-2
 Active: te1/0/1
 Inactive: po1-2
DHCP relay is enabled on VLANs: 1, 2, 4, 5
 Active: 1, 2, 4, 5
 Inactive:
Global Servers: 1.1.1.1 , 2.2.2.2
```

Example 4. Option 82 is supported (enabled) and there DHCP Servers defined per interface:

```
switchxxxxxx# show ip dhcp relay
DHCP relay is globally enabled
Option 82 is enabled
Maximum number of supported VLANs without IP Address is 4
Number of DHCP Relays enabled on VLANs without IP Address: 2
DHCP relay is enabled on Ports: te1/0/1,po1-2
 Active: te1/0/1
 Inactive: po1-2
DHCP relay is enabled on VLANs: 1, 2, 4, 5
 Active: 1, 2, 4, 5
 Inactive:
Global Servers: 1.1.1.1 , 2.2.2.2
VLAN 1: 1.1.1.1, 100.10.1.1 VLAN 2: 3.3.3.3, 4.4.4.4, 5.5.5.5
VLAN 10: 6.6.6.6
```

8.6. ip dhcp information option

Use the `ip dhcp information option` Global Configuration command to enable DHCP option-82 data insertion. Use the no form of this command to disable DHCP option-82 data insertion.

Syntax

- ip dhcp information option
- no ip dhcp information option

Parameters

N/A

Default Configuration

DHCP option-82 data insertion is disabled.

Command Mode

Global Configuration mode

User Guidelines

DHCP option 82 would be enabled only if DHCP snooping or DHCP relay are enabled.

Example

```
switchxxxxxx(config)# ip dhcp information option
```

8.7. show ip dhcp information option

The show ip dhcp information option EXEC mode command displays the DHCP Option 82 configuration.

Syntax

- show ip dhcp information option

Parameters

N/A

Default Configuration

N/A

Command Mode

User EXEC mode

Example

The following example displays the DHCP Option 82 configuration.

```
switchxxxxxx# show ip dhcp information option
Relay agent Information option is Enabled
```

9. DHCP Server Commands

9.1. address (DHCP Host)

To manually bind an IP address to a DHCP client, use the `address` command in DHCP Pool Host Configuration mode. To remove the IP address binding to the client, use the no form of this command.

Syntax

- address ip-address {mask | prefix-length} {client-identifier unique-identifier | hardware-address mac-address}
- no address

Parameters

- address - Specifies the client IP address.
- mask - Specifies the client network mask.
- prefix-length - Specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the client network mask. The prefix length must be preceded by a forward slash (/).
- unique-identifier - Specifies the distinct client identification in dotted hexadecimal notation. Each byte in a hexadecimal character string is two hexadecimal digits. Bytes are separated by a period or colon. For example, 01b7.0813.8811.66.
- mac-address - Specifies the client MAC address.

Default Configuration

No address are bound.

Command Mode

DHCP Pool Host Configuration mode

User Guidelines

To classify the DHCP client, DHCP server uses either the client identifier passed in Option 61, if the client-identifier keyword is configured or the client MAC address, if the hardware-address keyword is configured.

Example

The following example manually binds an IP address to a DHCP client.

```
switchxxxxxx(config)# ip dhcp pool host aaaa
switchxxxxxx(config-dhcp)# address 10.12.1.99 255.255.255.0 client-identifier
01b7.0813.8811.66
switchxxxxxx(config-dhcp)# exit
switchxxxxxx(config)# ip dhcp pool host bbbb
switchxxxxxx(config-dhcp)# address 10.12.1.88 255.255.255.0 hardware-address
00:01:b7:08:13:88
switchxxxxxx(config-dhcp)# exit
switchxxxxxx(config)#
```

9.2. address (DHCP Network)

To configure the subnet number and mask for a DHCP address pool on a DHCP server, use the `address` command in DHCP Pool Network Configuration mode. To remove the subnet number and mask, use the no form of this command.

Syntax

- address {network-number | low low-address high high-address} {mask | prefix-length}
- no address

Parameters

- network-number - Specifies the IP address of the DHCP address pool.
- mask - Specifies the pool network mask.
- prefix-length - Specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the client network mask. The prefix length must be preceded by a forward slash (/).
- low low-address - Specifies the first IP address to use in the address range.
- high high-address - Specifies the last IP address to use in the address range.

Default Configuration

DHCP address pools are not configured.

If the low address is not specified, it defaults to the first IP address in the network.

If the high address is not specified, it defaults to the last IP address in the network.

Command Mode

DHCP Pool Network Configuration mode

Example

The following example configures the subnet number and mask for a DHCP address pool on a DHCP server.

```
switchxxxxxx(config-dhcp)# address 10.12.1.0 255.255.255.0
```

9.3. bootfile

To specify the default boot image file name for a DHCP client, use the `bootfile` command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To delete the boot image file name, use the no form of this command.

Syntax

- bootfile filename
- no bootfile

Parameters

- filename - Specifies the file name used as a boot image. (Length: 1–128 characters).

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host Configuration mode

Example

The following example specifies boot_image_file as the default boot image file name for a DHCP client.

```
switchxxxxxx(config-dhcp)# bootfile boot_image_file
```

9.4. clear ip dhcp binding

To delete the dynamic address binding from the DHCP server database, use the `clear ip dhcp binding` command in Privileged EXEC mode.

Syntax

- clear ip dhcp binding {address | *}

Parameters

- address - Specifies the binding address to delete from the DHCP database.
- * - Clears all dynamic bindings.

Command Mode

Privileged EXEC mode

User Guidelines

Typically, the address supplied denotes the client IP address. If the asterisk (*) character is specified as the address parameter, DHCP clears all dynamic bindings.

Use the no ip dhcp pool Global Configuration mode command to delete a manual binding.

Example

The following example deletes the address binding 10.12.1.99 from a DHCP server database:

```
switchxxxxxx# clear ip dhcp binding 10.12.1.99
```

9.5. client-name

To define the name of a DHCP client, use the `client-name` command in DHCP Pool Host Configuration mode. To remove the client name, use the no form of this command.

Syntax

- client-name name
- no client-name

Parameters

- name - Specifies the client name, using standard ASCII characters.

Command Mode

DHCP Pool Host Configuration mode

Default Configuration

No client name is defined.

User Guidelines

It is possible to specify up to 512 clients.

The client name should not include the domain name. For example, the name “Bob” should not be specified as bob.domain.com. (Length: 1–32 characters).

Example

The following example defines the string client1 as the client name.

```
switchxxxxxx(config-dhcp)# client-name client1
```

9.6. default-router

To configure the default router list for a DHCP client, use the `default-router` command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the default router list, use the no form of this command.

Syntax

- default-router ip-address [ip-address2 ... ip-address8]
- no default-router

Parameters

- ip-address [ip-address2 ... ip-address8] - Specifies the IP addresses of default routers. Up to eight addresses can be specified in one command line.

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host Configuration mode

Default Configuration

No default router is defined.

User Guidelines

The router IP address should be on the same subnet as the client subnet.

The DHCP server returns an IP address defined on the input interface as a default router if an default router is not configured in the following case:

- Default router is not configurable.
- DHCP client is directly connected.
- IP Routing is enabled.
- Default router was required by the client.

Example

The following example specifies 10.12.1.99 as the default router IP address.

```
switchxxxxxx(config-dhcp)# default-router 10.12.1.99
```

9.7. dns-server

To configure the Domain Name System (DNS) IP server list available to a DHCP client, use the `dns-server` command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the DNS server list, use the no form of this command.

Syntax

- dns-server ip-address [ip-address2 ... ip-address8]
- no dns-server

Parameters

- ip-address [ip-address2 ... ip-address8] - Specifies the IP addresses of DNS servers. Up to eight addresses can be specified in one command line.

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host Configuration mode

Default Configuration

No DNS server is defined.

User Guidelines

If DNS IP servers are not configured for a DHCP client, the client cannot correlate host names to IP addresses.

Example

The following example specifies 10.12.1.99 as the client domain name server IP address.

```
switchxxxxxx(config-dhcp)# dns-server 10.12.1.99
```

9.8. domain-name

To specify the domain name for a DHCP client, use the `domain-name` command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the domain name, use the no form of this command.

Syntax

- domain-name domain
- no domain-name

Parameters

- domain - Specifies the DHCP client domain name string. (Length: 1–32 characters).

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host Configuration mode

Default Configuration

No domain name is defined.

Example

The following example specifies yahoo.com as the DHCP client domain name string.

```
switchxxxxxx(config-dhcp)# domain-name yahoo.com
```

9.9. ip dhcp excluded-address

To specify IP addresses that a DHCP server must not assign to DHCP clients, use the `ip dhcp excluded-address` command in Global Configuration mode. To remove the excluded IP addresses, use the no form of this command.

Syntax

- ip dhcp excluded-address low-address [high-address]
- no ip dhcp excluded-address low-address [high-address]

Parameters

- low-address - Specifies the excluded IP address, or first IP address in an excluded address range.
- high-address - (Optional) Specifies the last IP address in the excluded address range.

Default Configuration

All IP pool addresses are assignable.

Command Mode

Global Configuration mode

User Guidelines

The DHCP server assumes that all pool addresses can be assigned to clients. Use this command to exclude a single IP address or a range of IP addresses.

Example

The following example configures an excluded IP address range from 172.16.1.100 through 172.16.1.199.

```
switchxxxxxx(config)# ip dhcp excluded-address 172.16.1.100 172.16.1.199
```

9.10. ip dhcp pool host

To configure a DHCP static address on a DHCP server and enter the DHCP Pool

Host Configuration mode, use the `ip dhcp pool host` command in Global Configuration mode. To remove the address pool, use the no form of this command.

Syntax

- ip dhcp pool host name
- no ip dhcp pool host name

Parameters

- name - Specifies the DHCP address pool name. It can be either a symbolic string (such as Engineering) or an integer (such as 8). (Length: 1–32 characters).

Default Configuration

DHCP hosts are not configured.

Command Mode

Global Configuration mode

User Guidelines

During execution of this command, the configuration mode changes to the DHCP Pool Configuration mode. In this mode, the administrator can configure host parameters, such as the IP subnet number and default router list.

Example

The following example configures station as the DHCP address pool:

```
switchxxxxxx(config)# ip dhcp pool host station
switchxxxxxx(config-dhcp)#
```

9.11. ip dhcp pool network

To configure a DHCP address pool on a DHCP Server and enter DHCP Pool

Network Configuration mode, use the `ip dhcp pool network` command in Global Configuration mode. To remove the address pool, use the no form of this command.

Syntax

- ip dhcp pool network name
- no ip dhcp pool network name

Parameters

- name - Specifies the DHCP address pool name. It can be either a symbolic string (such as 'engineering') or an integer (such as 8). (Length: 1–32 characters).

Default Configuration

DHCP address pools are not configured.

Command Mode

Global Configuration mode

User Guidelines

During execution of this command, the configuration mode changes to DHCP Pool Network Configuration mode. In this mode, the administrator can configure pool parameters, such as the IP subnet number and default router list.

Example

The following example configures Pool1 as the DHCP address pool.

```
switchxxxxxx(config)# ip dhcp pool network Pool1
switchxxxxxx(config-dhcp)#
```

9.12. ip dhcp server

To enable the DHCP server features on the device, use the `ip dhcp server` command in Global Configuration mode. To disable the DHCP server, use the no form of this command.

Syntax

- ip dhcp server
- no ip dhcp server

Default Configuration

The DHCP server is disabled.

Command Mode

Global Configuration mode

Example

The following example enables the DHCP server on the device:

```
switchxxxxxx(config)# ip dhcp server
```

9.13. lease

To configure the time duration of the lease for an IP address that is assigned from a DHCP server to a DHCP client, use the `lease` command in DHCP Pool Network Configuration mode. To restore the default value, use the no form of this command.

Syntax

- lease days [hours [minutes]] | infinite
- no lease

Parameters

- days - Specifies the number of days in the lease.
- hours - (Optional) Specifies the number of hours in the lease. A days value must be supplied before configuring an hours value.
- minutes - (Optional) Specifies the number of minutes in the lease. A days value and an hours value must be supplied before configuring a minutes value.
- infinite - Specifies that the duration of the lease is unlimited.

Default Configuration

The default lease duration is 1 day.

Command Mode

DHCP Pool Network Configuration mode

Examples

The following example shows a 1-day lease.

```
switchxxxxxx(config-dhcp)# lease 1
```

The following example shows a one-hour lease.

```
switchxxxxxx(config-dhcp)# lease 0 1
```

The following example shows a one-minute lease.

```
switchxxxxxx(config-dhcp)# lease 0 0 1
```

The following example shows an infinite (unlimited) lease.

```
switchxxxxxx(config-dhcp)# lease infinite
```

9.14. netbios-name-server

To configure the NetBIOS Windows Internet Naming Service (WINS) server list that is available to Microsoft DHCP clients, use the `netbios-name-server` in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the NetBIOS name server list, use the no form of this command.

Syntax

- netbios-name-server ip-address [ip-address2 ... ip-address8]
- no netbios-name-server

Parameters

- ip-address [ip-address2 ... ip-address8] - Specifies the IP addresses of NetBIOS WINS name servers. Up to eight addresses can be specified in one command line.

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host Configuration mode

Default Configuration

No bios server is defined.

Example

The following example specifies the IP address of a NetBIOS name server available to the DHCP client.

```
switchxxxxxx(config-dhcp)# netbios-name-server 10.12.1.90
```

9.15. netbios-node-type

To configure the NetBIOS node type for Microsoft DHCP clients, use the `netbios-node-type` command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To return to default, use the no form of this command.

Syntax

- netbios-node-type {b-node | p-node | m-node | h-node}
- no netbios-node-type

Parameters

- b-node - Specifies the Broadcast NetBIOS node type.
- p-node - Specifies the Peer-to-peer NetBIOS node type.
- m-node - Specifies the Mixed NetBIOS node type. h-node - Specifies the Hybrid NetBIOS node type.

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host Configuration mode

Default Configuration

h-node (Hybrid NetBIOS node type).

Example

The following example specifies the client's NetBIOS type as mixed.

```
switchxxxxxx(config-dhcp)# netbios node-type m-node
```

9.16. next-server

To configure the next server (siaddr) in the boot process of a DHCP client, use the `next-server` command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the next server, use the no form of this command.

Syntax

- next-server ip-address
- no next-server

Parameters

- ip-address - Specifies the IP address of the next server in the boot process.

Default Configuration

If the next-server command is not used to configure a boot server list, the DHCP server uses inbound interface helper addresses as boot servers.

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host Configuration mode

User Guidelines

The client will connect, using the SCP/TFTP protocol, to this server in order to download the configuration file.

Example

The following example specifies 10.12.1.99 as the IP address of the next server:

```
switchxxxxxx(config-dhcp)# next-server 10.12.1.99
```

9.17. next-server-name

To configure the next server name (sname) in the boot process of a DHCP client, use the `next-server-name` command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the boot server name, use the no form of this command.

Syntax

- next-server-name name
- no next-server-name

Parameters

- name - Specifies the name of the next server in the boot process. (Length: 1–64 characters).

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host Configuration mode

Default Configuration

No next server name is defined.

User Guidelines

The client will connect, using the SCP/TFTP protocol, to this server in order to download the configuration file.

Example

The following example specifies www.bootserver.com as the name of the next server in the boot process of a DHCP client.

```
switchxxxxxx(config-dhcp)# next-server www.bootserver.com
```

9.18. option

To configure the DHCP server options, use the `option` command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the options, use the no form of this command.

Syntax

- option code {boolean {false | true} | integer value | ascii string | hex {string | none} | ip {address} | ip-list {ip-address1 [ip-address2 …]}} [description text]
- no option code

Parameters

- code - Specifies the DHCP option code. The supported values are defined in the User Guidelines.
- boolean {false | true} - Specifies a boolean value. The values are coded by integer values of one octet: 0 = false and 1 = true.
- integer value - Specifies an integer value. The option size depends on the option code.
- ascii string - Specifies a network virtual terminal (NVT) ASCII character string. ASCII character strings that contain white spaces must be delimited by quotation marks. The ASCII value is truncated to the first 160 characters entered.
- ip address - Specifies an IP address.
- ip-list {ip-address1 [ip-address2 ...]} - Specifies up to 8 IP addresses.
- hex string - Specifies dotted hexadecimal data. The hexadecimal value is truncated to the first 320 characters entered. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period, colon, or white space.
- hex none - Specifies the zero-length hexadecimal string.
- description text - User description

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host Configuration mode

User Guidelines

The option command enables defining any option that cannot be defined by other special CLI commands. A new definition of an option overrides the previous definition of this option.

The boolean keyword may be configured for the following options: 19, 20, 27, 29-31, 34, 36, and 39.

The integer keyword may be configured for the following options: 2, 13, 22-26, 35, 37-38, 132-134, and 211. The switch checks the value range and builds the value field of the size in accordance with the option definition.

The ascii keyword may be configured for the following options: 14, 17-18, 40, 64, 130, 209, and 210.

The ip keyword may be configured for the following options: 16, 28, 32, 128-129, 131, 135, and 136.

The ip-list keyword may be configured for the following options: 5, 7-11, 33, 41, 42, 45, 48, 49, 65, 68-76, and 150.

The hex keyword may be configured for any option in the range 1-254 except for the following: 1, 3-4, 6, 12, 15, 44, 46, 50-51, 53-54, 56, 66-67, 82, and 255. The switch does not validate the Syntax of an option defined by this format.

Examples

Example 1. The following example configures DHCP option 19, which specifies whether the client should configure its IP layer for packet forwarding:

```
switchxxxxxx(config-dhcp)# option 19 boolean true description "IP Forwarding
Enable/Disable Option"
```

Example 2. The following example configures DHCP option 2, which specifies the offset of the client in seconds from Coordinated Universal Time (UTC):

```
switchxxxxxx(config-dhcp)# option 2 integer 3600
```

Example 3. The following example configures DHCP option 72, which specifies the World Wide Web servers for DHCP clients. World Wide Web servers 172.16.3.252 and 172.16.3.253 are configured in the following example:

```
switchxxxxxx(config-dhcp)# option 72 ip-list 172.16.3.252 172.16.3.253
```

9.19. show ip dhcp

To display the DHCP configuration, use the `show ip dhcp` command in User EXEC mode.

Syntax

- show ip dhcp

Command Mode

User EXEC mode

Example

The following example displays the DHCP configuration.

```
switchxxxxxx# show ip dhcp DHCP server is enabled.
```

9.20. show ip dhcp allocated

To display the allocated address or all the allocated addresses on the DHCP server, use the `show ip dhcp allocated` command in User EXEC mode.

Syntax

- show ip dhcp allocated [ip-address]

Parameters

- ip-address - (Optional) Specifies the IP address.

Command Mode

User EXEC mode

Example

The following example displays the output of various forms of this command:

```
switchxxxxxx# show ip dhcp allocated
DHCP server enabled
The number of allocated entries is 3
IP address Hardware address Lease expiration Type
---------- ---------------- -------------------- ---------
172.16.1.11 00a0.9802.32de Feb 01 1998 12:00 AM Dynamic
172.16.3.253 02c7.f800.0422 Infinite Automatic 172.16.3.254 02c7.f800.0422
Infinite Static
switchxxxxxx# show ip dhcp allocated 172.16.1.11
DHCP server enabled
The number of allocated entries is 2
IP address Hardware address Lease expiration Type
---------- ---------------- -------------------- -------172.16.1.11
00a0.9802.32de Feb 01 1998 12:00 AM Dynamic
switchxxxxxx# show ip dhcp allocated 172.16.3.254
```

```
DHCP server enabled
The number of allocated entries is 2
IP address Hardware address Lease expiration Type
---------- ---------------- -------------------- -------
172.16.3.254 02c7.f800.0422 Infinite Static
```

The following table describes the significant fields shown in the display.

Field	Description
IP address	The host IP address as recorded on the DHCP Server.
Hardware address	The MAC address or client identifier of the host as recorded on the DHCP Server.
Lease expiration	The lease expiration date of the host IP address.
Type	The manner in which the IP address was assigned to the host.

9.21. show ip dhcp binding

To display the specific address binding or all the address bindings on the DHCP server, use the `show ip dhcp binding` command in User EXEC mode.

Syntax

- show ip dhcp binding [ip-address]

Parameters

- ip-address - (Optional) Specifies the IP address.

Command Mode

User EXEC mode

Examples

The following examples display the DHCP server binding address parameters.

```
switchxxxxxx# show ip dhcp binding
DHCP server enabled
The number of used (all types) entries is 6
The number of pre-allocated entries is 1
The number of allocated entries is 1
The number of expired entries is 1
The number of declined entries is 2
The number of static entries is 1
The number of dynamic entries is 2
The number of automatic entries is 1
IP address Client Identifier Lease Expiration Type State
---------- ----------------- ------------- ------- ---------
1.16.1.11 00a0.9802.32de Feb 01 1998 dynamic allocated
1.16.3.23 02c7.f801.0422 12:00AM dynamic expired
1.16.3.24 02c7.f802.0422 dynamic declined
1.16.3.25 02c7.f803.0422 dynamic pre-allocated 1.16.3.26 02c7.f804.0422 dynamic
declined
switchxxxxxx# show ip dhcp binding 1.16.1.11
```

```
DHCP server enabled
IP address Client Identifier Lease Expiration Type State
---------- ----------------- ----------------- ------- ---------
1.16.1.11 00a0.9802.32de Feb 01 1998 dynamic allocated 12:00 AM
switchxxxxxx# show ip dhcp binding 1.16.3.24
IP address Client Identifier Lease Expiration Type State
---------- ----------------- --------------- ------- ---------
1.16.3.24 02c7.f802.0422 dynamic declined
```

The following table describes the significant fields shown in the display.

Field	Description
IP address	The host IP address as recorded on the DHCP Server.
Client Identifier	The MAC address or client identifier of the host as recorded on the DHCP Server.
Lease expiration	The lease expiration date of the host IP address.
Field	Description
Type	The manner in which the IP address was assigned to the host.
State	The IP Address state.

9.22. show ip dhcp declined

To display the specific declined address or all of the declined addresses on the DHCP server, use the `show ip dhcp declined` command in User EXEC mode.

Syntax

- show ip dhcp declined [ip-address]

Parameters

- ip-address - (Optional) Specifies the IP address.

Command Mode

User EXEC mode

Example

The following example displays the output of various forms of this command:

```
switchxxxxxx# show ip dhcp declined
DHCP server enabled
The number of declined entries is 2
IP address Hardware address
172.16.1.11 00a0.9802.32de 172.16.3.254 02c7.f800.0422
switchxxxxxx# show ip dhcp declined 172.16.1.11
DHCP server enabled
The number of declined entries is 2
IP address Hardware address
172.16.1.11 00a0.9802.32de
```

9.23. show ip dhcp excluded-addresses

To display the excluded addresses, use the `show ip dhcp excluded-addresses` command in User EXEC mode.

Syntax

- show ip dhcp excluded-addresses

Command Mode

User EXEC mode

Example

The following example displays excluded addresses.

```
switchxxxxxx# show ip dhcp excluded-addresses
The number of excluded addresses ranges is 2 Excluded addresses:
10.1.1.212- 10.1.1.219, 10.1.2.212- 10.1.2.219
```

9.24. show ip dhcp expired

To display the specific expired address or all of the expired addresses on the DHCP server, use the `show ip dhcp expired` command in User EXEC mode.

Syntax

- show ip dhcp expired [ip-address]

Parameters

- ip-address - (Optional) Specifies the IP.

Command Mode

User EXEC mode

Example

```
switchxxxxxx# show ip dhcp expired
DHCP server enabled
The number of expired entries is 1
IP address Hardware address
172.16.1.11 00a0.9802.32de 172.16.3.254 02c7.f800.0422
switchxxxxxx# show ip dhcp expired 172.16.1.11
DHCP server enabled
The number of expired entries is 1
IP address Hardware address
172.16.1.13 00a0.9802.32de
```

9.25. show ip dhcp pool host

To display the DHCP pool host configuration, use the `show ip dhcp pool host` command in User EXEC mode.

Syntax

- show ip dhcp pool host [address | name]

Parameters

- address - (Optional) Specifies the client IP address.

- name - (Optional) Specifies the DHCP pool name. (Length: 1-32 characters)

Command Mode

User EXEC mode

Examples

Example 1. The following example displays the configuration of all DHCP host pools:

```
switchxxxxxx# show ip dhcp pool host
The number of host pools is 1
Name IP Address Hardware Address Client Identifier ---------- ---------- -------
--------- ----------------station 172.16.1.11 01b7.0813.8811.66
```

Example 2. The following example displays the DHCP pool host configuration of the pool named station:

```
switchxxxxxx# show ip dhcp pool host station
Name IP Address Hardware Address Client Identifier ---------- ---------- -------
--------- ----------------station 172.16.1.11 01b7.0813.8811.66
Mask: 255.255.0.0
Default router: 172.16.1.1
Client name: client1
DNS server: 10.12.1.99 Domain name: yahoo.com
NetBIOS name server: 10.12.1.90
NetBIOS node type: h-node
Next server: 10.12.1.99
Next-server-name: 10.12.1.100
Bootfile: Bootfile Time server 10.12.1.99 Options:
Code Type Len Value Description
--- ------- --- ---------------- --------------------------------
2 integer 4 3600
14 ascii 16 qq/aaaa/bbb.txt
19 boolean 1 false "IP Forwarding Enable/Disable
  Option"
21 ip 4 134.14.14.1
31 ip-list 8 1.1.1.1, 12.23.45.2
47 hex 5 02af00aa00
```

9.26. show ip dhcp pool network

To display the DHCP network configuration, use the `show ip dhcp pool network` command in User EXEC mode.

Syntax

- show ip dhcp pool network [name]

Parameters

- name - (Optional) Specifies the DHCP pool name. (Length: 1-32 characters).

Command Mode

User EXEC mode

Examples

Example 1 - The following example displays configuration of all DHCP network pools:

```
switchxxxxxx# show ip dhcp pool network
```

```
The number of network pools is 2
Name Address range mask Lease
------------------------------------------------- marketing 10.1.1.17-
10.1.1.178 255.255.255.0 0d:12h:0m finance 10.1.2.8-10.1.2.178 255.255.255.0
0d:12h:0m
```

Example 2 - The following example displays configuration of the DHCP network pool marketing:

```
switchxxxxxx# show ip dhcp pool network marketing
Name Address range mask Lease
-------------------------------- ----------------------marketing 10.1.1.17-
10.1.1.178 255.255.255.0 0d:12h:0m
Statistics:
All-range Available Free Pre-allocated Allocated Expired Declined
---------- --------- ----- ------------ --------- --------- --------
162 150 68 50 20 3 9
Default router: 10.1.1.1
DNS server: 10.12.1.99
Domain name: yahoo.com
NetBIOS name server: 10.12.1.90
NetBIOS node type: h-node
Next server: 10.12.1.99
Next-server-name: 10.12.1.100
Bootfile: Bootfile Time server 10.12.1.99
Options:
Code Type Len Value Description
--- ------- --- -------------------- -------------------------------
2 integer 4 3600
14 ascii 16 qq/aaaa/bbb.txt
19 boolean 1 false "IP Forwarding Enable/Disable
  Option"
21 ip 4 134.14.14.1
31 ip-list 8 1.1.1.1, 12.23.45.2
47 hex 5 02af00aa00
```

9.27. show ip dhcp pre-allocated

To display the specific pre-allocated address or all the pre-allocated addresses on the DHCP server, use the `show ip dhcp pre-allocated` command in User EXEC mode.

Syntax

- show ip dhcp pre-allocated [ip-address]

Parameters

- ip-address - (Optional) Specifies the IP.

Command Mode

User EXEC mode

Examples

```
switchxxxxxx# show ip dhcp pre-allocated
DHCP server enabled
The number of pre-allocated entries is 1
IP address Hardware address
```

```
172.16.1.11 00a0.9802.32de 172.16.3.254 02c7.f800.0422
switchxxxxxx# show ip dhcp pre-allocated 172.16.1.11
DHCP server enabled
The number of pre-allocated entries is 1
IP address Hardware address
172.16.1.15 00a0.9802.32de
```

9.28. show ip dhcp server statistics

To display DHCP server statistics, use the `show ip dhcp server statistics` command in User EXEC mode.

Syntax

- show ip dhcp server statistics

Command Mode

User EXEC mode

Example

The following example displays DHCP server statistics

```
switchxxxxxx# show ip dhcp server statistics
DHCP server enabled
The number of network pools is 7
The number of excluded pools is 2
The number of used (all types) entries is 7
The number of pre-allocated entries is 1
The number of allocated entries is 3
The number of expired entries is 1
The number of declined entries is 2
The number of static entries is 1
The number of dynamic entries is 2
The number of automatic entries is 1
```

9.29. time-server

To specify the time servers list for a DHCP client, use the `time-server` command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the time servers list, use the no form of this command.

Syntax

- time-server ip-address [ip-address2 ... ip-address8]
- no time-server

Parameters

- ip-address [ip-address2 ... ip-address8] - Specifies the IP addresses of Time servers. Up to eight addresses can be specified in one command line.

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host Configuration mode

Default Configuration

No time server is defined.

User Guidelines

The time server’s IP address should be on the same subnet as the client subnet.

Example

The following example specifies 10.12.1.99 as the time server IP address.

```
switchxxxxxx(config-dhcp)# time-server 10.12.1.99
```

10. DHCP Relay Commands

10.1. ip dhcp relay enable (Global)

Use the `ip dhcp relay enable` Global Configuration mode command to enable the DHCP relay feature on the device. Use the `no` form of this command to disable the DHCP relay feature.

Syntax

- ip dhcp relay enable
- no ip dhcp relay enable

Parameters

N/A

Default Configuration

DHCP relay feature is disabled.

Command Mode

Global Configuration mode

Example

The following example enables the DHCP relay feature on the device:

```
switchxxxxxx(config)# ip dhcp relay enable
```

10.2. ip dhcp relay enable (Interface)

Use the `ip dhcp relay enable` Interface Configuration mode command to enable the DHCP relay feature on an interface. Use the `no` form of this command to disable the DHCP relay agent feature on an interface.

Syntax

- ip dhcp relay enable
- no ip dhcp relay enable

Parameters

N/A

Default Configuration

Disabled

Command Mode

Interface Configuration mode

User Guidelines

The operational status of DHCP Relay on an interface is active if one of the following conditions exist:

- DHCP Relay is globally enabled, and there is an IP address defined on the interface.

or

- DHCP Relay is globally enabled, there is no IP address defined on the interface, the interface is a VLAN, and option 82 is enabled.

Example

The following example enables DHCP Relay on VLAN 21:

```
switchxxxxxx(config)# interface vlan 21
switchxxxxxx(config-if)# ip dhcp relay enable
```

10.3. ip dhcp relay address (Global)

Use the `ip dhcp relay address` Global Configuration mode command to define the DHCP servers available for the DHCP relay. Use the `no` form of this command to remove the server from the list.

Syntax

- ip dhcp relay address ip-address
- no ip dhcp relay address [ip-address]

Parameters

- ip-address - Specifies the DHCP server IP address. Up to 8 servers can be defined.

Default Configuration

No server is defined.

Command Mode

Global Configuration mode

User Guidelines

Use the `ip dhcp relay address` command to define a global DHCP Server IP address. To define a few DHCP Servers, use the command a few times.

To remove a DHCP Server, use the no form of the command with the ip-address argument.

The no form of the command without the ip-address argument deletes all global defined DHCP servers.

Example

The following example defines the DHCP server on the device.

```
switchxxxxxx(config)# ip dhcp relay address 176.16.1.1
```

10.4. ip dhcp relay address (Interface)

Use the `ip dhcp relay address` Interface Configuration (VLAN, Ethernet, Port-channel) command to define the DHCP servers available by the DHCP relay for DHCP clients connected to the interface. Use the no form of this command to remove the server from the list.

Syntax

- ip dhcp relay address ip-address
- no ip dhcp relay address [ip-address]

Parameters

- ip-address - Specifies the DHCP server IP address. Up to 8 servers can be defined.

Default Configuration

No server is defined.

Command Mode

Interface Configuration mode

User Guidelines

Use the `ip dhcp relay address` command to define a DHCP Server IP address per the interface. To define multiple DHCP Servers, use the command multiple times.

To remove a DHCP server, use the no form of the command with the ip-address argument.

The no form of the command without the ip-address argument deletes all DHCP servers.

Example

The following example defines the DHCP server on the device.

```
switchxxxxxx(config)# interface vlan 21
switchxxxxxx(config-if)# ip dhcp relay address 176.16.1.1
```

10.5. show ip dhcp relay

Use the `show ip dhcp relay` EXEC mode command to display the DHCP relay information.

Syntax

- show ip dhcp relay

Command Mode

User EXEC mode

Examples

Example 1: Option 82 is not supported:

```
switchxxxxxx# show ip dhcp relay
DHCP relay is globally enabled
Option 82 is Disabled
Maximum number of supported VLANs without IP Address is 256
Number of DHCP Relays enabled on VLANs without IP Address is 0
DHCP relay is not configured on any port.
DHCP relay is not configured on any vlan.
No servers configured
```

Example 2: Option 82 is supported (disabled):

```
switchxxxxxx# show ip dhcp relay
DHCP relay is globally disabled
Option 82 is disabled
Maximum number of supported VLANs without IP Address: 0
Number of DHCP Relays enabled on VLANs without IP Address: 4
DHCP relay is enabled on Ports: te1/0/1,po1-2
  Active:
  Inactive: te1/0/1, po1-4
DHCP relay is enabled on VLANs: 1, 2, 4, 5
  Active:
  Inactive: 1, 2, 4, 5
```

```
Global Servers: 1.1.1.1 , 2.2.2.2
```

Example 3: Option 82 is supported (enabled):

```
switchxxxxxx# show ip dhcp relay
DHCP relay is globally enabled
Option 82 is enabled
Maximum number of supported VLANs without IP Address is 4
Number of DHCP Relays enabled on VLANs without IP Address: 2
DHCP relay is enabled on Ports: te1/0/1,po1-2
  Active: te1/0/1
  Inactive: po1-2
DHCP relay is enabled on VLANs: 1, 2, 4, 5
  Active: 1, 2, 4, 5
  Inactive:
Global Servers: 1.1.1.1 , 2.2.2.2
```

Example 4: Option 82 is supported (enabled) and there DHCP Servers defined per interface:

```
switchxxxxxx# show ip dhcp relay
DHCP relay is globally enabled
Option 82 is enabled
Maximum number of supported VLANs without IP Address is 4
Number of DHCP Relays enabled on VLANs without IP Address: 2
DHCP relay is enabled on Ports: te1/0/1,po1-2
  Active: te1/0/1
  Inactive: po1-2
DHCP relay is enabled on VLANs: 1, 2, 4, 5
  Active: 1, 2, 4, 5
  Inactive:
Global Servers: 1.1.1.1 , 2.2.2.2
VLAN 1: 1.1.1.1, 100.10.1.1
VLAN 2: 3.3.3.3, 4.4.4.4, 5.5.5.5
VLAN 10: 6.6.6.6
```

10.6. ip dhcp information option

Use the `ip dhcp information option` Global Configuration command to enable DHCP option-82 data insertion. Use the no form of this command to disable DHCP option-82 data insertion.

Syntax

- ip dhcp information option
- no ip dhcp information option

Parameters

N/A

Default Configuration

DHCP option-82 data insertion is disabled.

Command Mode

Global Configuration mode

User Guidelines

DHCP option 82 would be enabled only if DHCP snooping or DHCP relay are enabled.

Example

```
switchxxxxxx(config)# ip dhcp information option
```

10.7. show ip dhcp information option

The `show ip dhcp information option` EXEC mode command displays the DHCP Option 82 configuration.

Syntax

- show ip dhcp information option

Parameters

N/A

Default Configuration

N/A

Command Mode

User EXEC mode

Example

The following example displays the DHCP Option 82 configuration.

```
switchxxxxxx# show ip dhcp information option
Relay agent Information option is Enabled
```

11. DHCP Snooping Commands

11.1. ip dhcp snooping

Use the `ip dhcp snooping` Global Configuration mode command to enable Dynamic Host Configuration Protocol (DHCP) Snooping globally. Use the no form of this command to restore the default configuration.

Syntax

- ip dhcp snooping
- no ip dhcp snooping

Parameters

N/A

Default Configuration

DHCP snooping is disabled.

Command Mode

Global Configuration mode

User Guidelines

For any DHCP Snooping configuration to take effect, DHCP Snooping must be enabled globally. DHCP Snooping on a VLAN is not active until DHCP Snooping on a VLAN is enabled by using the `ip dhcp snooping vlan` Global Configuration mode command.

Example

The following example enables DHCP Snooping on the device.

```
switchxxxxxx(config)# ip dhcp snooping
```

11.2. ip dhcp snooping vlan

Use the `ip dhcp snooping vlan` Global Configuration mode command to enable DHCP Snooping on a VLAN. Use the no form of this command to disable DHCP Snooping on a VLAN.

Syntax

- ip dhcp snooping vlan vlan-id
- no ip dhcp snooping vlan vlan-id

Parameters

- vlan-id - Specifies the VLAN ID (up to 77 VLANs)

Default Configuration

DHCP Snooping on a VLAN is disabled.

Command Mode

Global Configuration mode

User Guidelines

DHCP Snooping must be enabled globally before enabling DHCP Snooping on a VLAN.

Example

The following example enables DHCP Snooping on VLAN 21.

```
switchxxxxxx(config)# ip dhcp snooping vlan 21
```

11.3. ip dhcp snooping trust

Use the `ip dhcp snooping trust` Interface Configuration (Ethernet, Port-channel) mode command to configure a port as trusted for DHCP snooping purposes. Use the no form of this command to restore the default configuration.

Syntax

- ip dhcp snooping trust
- no ip dhcp snooping trust

Parameters

N/A

Default Configuration

The interface is untrusted.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Configure as trusted the ports that are connected to a DHCP server or to other switches or routers. Configure the ports that are connected to DHCP clients as untrusted.

Example

The following example configures te1/0/4 as trusted for DHCP Snooping.

```
switchxxxxxx(config)# interface te1/0/4
switchxxxxxx(config-if)# ip dhcp snooping trust
```

11.4. ip dhcp snooping information option allowed-untrusted

Use the `ip dhcp snooping information option allowed-untrusted` Global Configuration mode command to allow a device to accept DHCP packets with option-82 information from an untrusted port. Use the no form of this command to drop these packets from an untrusted port.

Syntax

- ip dhcp snooping information option allowed-untrusted
- no ip dhcp snooping information option allowed-untrusted

Parameters

N/A

Default Configuration

DHCP packets with option-82 information from an untrusted port are discarded.

Command Mode

Global Configuration mode

Example

The following example allows a device to accept DHCP packets with option-82 information from an untrusted port.

```
switchxxxxxx(config)# ip dhcp snooping information option allowed-untrusted
```

11.5. ip dhcp snooping verify

Use the `ip dhcp snooping verify` Global Configuration mode command to configure a device to verify that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address. Use the no form of this command to disable MAC address verification in a DHCP packet received on an untrusted port.

Syntax

- ip dhcp snooping verify
- no ip dhcp snooping verify

Default Configuration

The switch verifies that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address in the packet.

Command Mode

Global Configuration mode

Example

The following example configures a device to verify that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address.

```
switchxxxxxx(config)# ip dhcp snooping verify
```

11.6. ip dhcp snooping database

Use the `ip dhcp snooping database` Global Configuration mode command to enable the DHCP Snooping binding database file. Use the no form of this command to delete the DHCP Snooping binding database file.

Syntax

- ip dhcp snooping database
- no ip dhcp snooping database

Parameters

N/A

Default Configuration

The DHCP Snooping binding database file is not defined.

Command Mode

Global Configuration mode

User Guidelines

The DHCP Snooping binding database file resides on Flash.

To ensure that the lease time in the database is accurate, the Simple Network Time Protocol (SNTP) must be enabled and configured.

The device writes binding changes to the binding database file only if the device system clock is synchronized with SNTP.

Example

The following example enables the DHCP Snooping binding database file.

```
switchxxxxxx(config)# ip dhcp snooping database
```

11.7. ip dhcp snooping binding

Use the `ip dhcp snooping binding` Privileged EXEC mode command to configure the DHCP Snooping binding database and add dynamic binding entries to the database. Use the no form of this command to delete entries from the binding database.

Syntax

- ip dhcp snooping binding mac-address vlan-id ip-address interface-id expiry {seconds | infinite}
- no ip dhcp snooping binding mac-address vlan-id

Parameters

- mac-address - Specifies a MAC address.
- vlan-id - Specifies a VLAN number.
- ip-address - Specifies an IP address.
- interface-id - Specifies an interface ID. The interface ID can be one of the following types:
  - Ethernet port
  - Port-channel.
- expiry
  - seconds - Specifies the time interval, in seconds, after which the binding entry is no longer valid. (Range: 10–4294967294).
  - infinite - Specifies infinite lease time.

Default Configuration

No static binding exists.

Command Mode

Privileged EXEC mode

User Guidelines

Use the `ip dhcp snooping binding` command to add manually a dynamic entry to the DHCP database.

After entering this command, an entry is added to the DHCP Snooping database. If the DHCP Snooping binding file exists, the entry is also added to that file.

The entry would not be added to the configuration files. The entry would be displayed in the show commands as a “DHCP Snooping” entry.

An entry added by this command can override the existed dynamic entry.

An entry added by this command cannot override the existed static entry added by the `ip source-guard binding` command.

The entry is displayed in the show commands as a DHCP Snooping entry.

Use the `no ip dhcp snooping binding` command to delete manually a dynamic entry from the DHCP database.

A dynamic temporary entries for which the IP address is 0.0.0.0 cannot be deleted.

Example

The following example adds a binding entry to the DHCP Snooping binding database.

```
switchxxxxxx# ip dhcp snooping binding 0060.704C.73FF 23 176.10.1.1 te1/0/4
expiry 900
```

11.8. clear ip dhcp snooping database

Use the `clear ip dhcp snooping database` Privileged EXEC mode command to clear the DHCP Snooping binding database.

Syntax

- clear ip dhcp snooping database

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

The following example clears the DHCP Snooping binding database.

```
switchxxxxxx# clear ip dhcp snooping database
```

11.9. show ip dhcp snooping

Use the `show ip dhcp snooping` EXEC mode command to display the DHCP snooping configuration for all interfaces or for a specific interface.

Syntax

- show ip dhcp snooping [interface-id]

Parameters

- interface-id - Specifies an interface ID. The interface ID can be one of the following types:
  - Ethernet port
  - Port-channel.

Command Mode

User EXEC mode

Example

The following example displays the DHCP snooping configuration.

```
switchxxxxxx# show ip dhcp snooping
DHCP snooping is Enabled
DHCP snooping is configured on following VLANs: 21
DHCP snooping database is Enabled
```

```
Relay agent Information option 82 is Enabled
Option 82 on untrusted port is allowed
Verification of hwaddr field is Enabled
DHCP snooping file update frequency is configured to: 6666 seconds
Interface Trusted
-------- -------
te1/0/1 Yes
te1/0/2 Yes
```

11.10. show ip dhcp snooping binding

Use the `show ip dhcp snooping binding` User EXEC mode command to display the DHCP Snooping binding database and configuration information for all interfaces or for a specific interface.

Syntax

- show ip dhcp snooping binding [mac-address mac-address] [ip-address ip-address] [vlan vlan-id] [interface-id]

Parameters

- mac-address mac-address - Specifies a MAC address.
- ip-address ip-address - Specifies an IP address.
- vlan vlan-id - Specifies a VLAN ID.
- interface-id - Specifies an interface ID. The interface ID can be one of the following types:
  - Ethernet port
  - Port-channel.

Command Mode

User EXEC mode

Example

The following examples displays the DHCP snooping binding database and configuration information for all interfaces on a device.-

```
switchxxxxxx# show ip dhcp snooping binding
Update frequency: 1200
Total number of binding: 2
Mac Address IP Address Lease Type VLAN Interface
 (sec)
-------------- ---------- ----- ----- ---- ---------
0060.704C.73FF 10.1.8.1 7983 snooping 3 te1/0/1
0060.704C.7BC1 10.1.8.2 92332 snooping (s) 3 te1/0/2
```

11.11. ip source-guard

Use the `ip source-guard` command in Configuration mode or Interface

Configuration mode to enable IP Source Guard globally on a device or in Interface Configuration (Ethernet, Port-channel) mode to enable IP Source Guard on an interface.

Use the no form of this command to disable IP Source Guard on the device or on an interface.

Syntax

- ip source-guard

- no ip source-guard

Parameters

N/A

Default Configuration

IP Source Guard is disabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration modeIP Source Guard must be enabled globally before enabling IP Source Guard on an interface.

IP Source Guard is active only on DHCP snooping untrusted interfaces, and if at least one of the interface VLANs are DHCP snooping enabled.

Example

The following example enables IP Source Guard on te1/0/4.

```
switchxxxxxx(config)# interface te1/0/4
switchxxxxxx(config-if)# ip source-guard
```

11.12. ip source-guard binding

Use the `ip source-guard binding` Global Configuration mode command to configure the static IP source bindings on the device. Use the no form of this command to delete the static bindings.

Syntax

- ip source-guard binding mac-address vlan-id ip-address interface-id
- no ip source-guard binding mac-address vlan-id

Parameters

- mac-address - Specifies a MAC address.
- vlan-id - Specifies a VLAN number.
- ip-address - Specifies an IP address.
- interface-id - Specifies an interface ID. The interface ID can be one of the following types
  - Ethernet port
  - Port-channel.

Default Configuration

No static binding exists.

Command Mode

Global Configuration mode

Use the `ip source-guard binding` command to add a static entry to the DHCP database.

An entry added by this command can override the existed entry.

Use the `no ip source-guard binding` command to delete an entry from the DHCP database.

Example

The following example configures the static IP source bindings.

```
switchxxxxxx(config)# ip source-guard binding 0060.704C.73FF 23 176.10.1.1
te1/0/4
```

11.13. ip source-guard tcam retries-freq

Use the `ip source-guard tcam retries-freq` Global Configuration mode command to set the frequency of retries for TCAM resources for inactive IP Source Guard addresses. Use the no form of this command to restore the default configuration.

Syntax

- ip source-guard tcam retries-freq {seconds | never}
- no ip source-guard tcam retries-freq

Parameters

- seconds - Specifies the retries frequency in seconds. (Range: 10–600)
- never - Disables automatic searching for TCAM resources.

Default Configuration

The default retries frequency is 60 seconds.

Command Mode

Global Configuration mode

Since the IP Source Guard uses the Ternary Content Addressable Memory (TCAM) resources, there may be situations when IP Source Guard addresses are inactive because of a lack of TCAM resources.

By default, once every minute the software conducts a search for available space in the TCAM for the inactive IP Source Guard addresses. Use this command to change the search frequency or to disable automatic retries for TCAM space.

The `ip source-guard tcam locate` command manually retries locating TCAM resources for the inactive IP Source Guard addresses.

The `show ip source-guard inactive` EXEC mode command displays the inactive IP Source Guard addresses.

Example

The following example sets the frequency of retries for TCAM resources to 2 minutes.

```
switchxxxxxx(config)# ip source-guard tcam retries-freq 120
```

11.14. ip source-guard tcam locate

Use the `ip source-guard tcam locate` Privileged EXEC mode command to manually retry to locate TCAM resources for inactive IP Source Guard addresses.

Syntax

- ip source-guard tcam locate

Parameters

N/A

Command Mode

Privileged EXEC mode

User Guidelines

Since the IP Source Guard uses the Ternary Content Addressable Memory (TCAM) resources, there may be situations when IP Source Guard addresses are inactive because of a lack of TCAM resources.

By default, once every 60 seconds the software conducts a search for available space in the TCAM for the inactive IP Source Guard addresses.

Execute the `ip source-guard tcam retries-freq` command with the never keyword to disable automatic retries for TCAM space, and then execute this command to manually retry locating TCAM resources for the inactive IP Source Guard addresses.

The `show ip source-guard inactive` EXEC mode command displays the inactive IP source guard addresses.

Example

The following example manually retries to locate TCAM resources.

```
switchxxxxxx# ip source-guard tcam locate
```

11.15. show ip source-guard configuration

Use the `show ip source-guard configuration` EXEC mode command to display the IP source guard configuration for all interfaces or for a specific interface.

Syntax

- show ip source-guard configuration [interface-id]

Parameters

- interface-id - Specifies an interface ID. The interface ID can be one of the following types:
  - Ethernet port
  - Port-channel.

Command Mode User EXEC mode Example

The following example displays the IP Source Guard configuration.

```
switchxxxxxx# show ip source-guard configuration
IP source guard is globally enabled.
Interface State
-------- -------
te1/0/1 Enabled
te1/0/2 Enabled
te1/0/3 Enabled
te1/0/4 Enabled
```

11.16. show ip source-guard status

Use the `show ip source-guard status` EXEC mode command to display the IP Source Guard status.

Syntax

- show ip source-guard status [mac-address mac-address] [ip-address ip-address] [vlan vlan] [interface-id]

Parameters

- mac-address mac-address - Specifies a MAC address.
- ip-address ip-address - Specifies an IP address.
- vlan vlan-id - Specifies a VLAN ID.
- interface-id - Specifies an interface ID. The interface ID can be one of the following types:
  - Ethernet port
  - Port-channel.

Command Mode User EXEC mode Example

The following examples display the IP Source Guard status.

```
switchxxxxxx# show ip source-guard status
IP source guard is globally enabled.
Interface Filter Status IP Address MAC Address VLAN Type
--------- ------ ------ ---------- ----------- ---- ----
te1/0/1 IP Active 10.1.8.1 0060.704C.73FF 3 DHCP
te1/0/2 IP Active 10.1.8.2 0060.704C.7BC1 3 Static
te1/0/3 IP Active Deny all 0060.704C.7BC3 4 DHCP
te1/0/4 IP Inactive
```

11.17. show ip source-guard inactive

Use the `show ip source-guard inactive` EXEC mode command to display the IP Source Guard inactive addresses.

Syntax

- show ip source-guard inactive

Parameters

N/A

Command Mode

User EXEC mode

User Guidelines

Since the IP Source Guard uses the Ternary Content Addressable Memory (TCAM) resources, there may be situations when IP Source Guard addresses are inactive because of a lack of TCAM resources.

By default, once every minute the software conducts a search for available space in the TCAM for the inactive IP Source Guard addresses.

Use the `ip source-guard tcam retries-freq` command to change the retry frequency or to disable automatic retries for TCAM space.

Use the `ip source-guard tcam locate` command to manually retry locating TCAM resources for the inactive IP Source Guard addresses.

This command displays the inactive IP source guard addresses.

Example

The following example displays the IP source guard inactive addresses.

```
switchxxxxxx# show ip source-guard inactive
TCAM resources search frequency: 60 seconds
Interface Filter IP MAC Address VLAN Type Reason
 Address
--------- ------ ------- ----------- ---- ---- ------
te1/0/2 IP 10.1.8.32 0060.704C.8 3 DHCP Resource
te1/0/3 IP 3FF Problem
te1/0/4 IP  Trust port
```

11.18. show ip source-guard statistics

Use the `show ip source-guard statistics` EXEC mode command to display the Source Guard dynamic information (permitted stations).

Syntax

- show ip source-guard statistics [vlan vlan-id]

Parameters

- vlan-id - Display the statistics on this VLAN.

Command Mode

User EXEC mode

Example

```
switchxxxxxx# show ip source-guard statistics
VLAN Statically Permitted Stations DHCP Snooping Permitted Stations
---- ------------------------------ --------------------------------
2 2 3
```

11.19. ip arp inspection

Use the `ip arp inspection` Global Configuration mode command globally to enable Address Resolution Protocol (ARP) inspection. Use the no form of this command to disable ARP inspection.

Syntax

- ip arp inspection
- no ip arp inspection

Parameters

N/A

Default Configuration

ARP inspection is disabled.

Command Mode

Global Configuration mode

User Guidelines

Note that if a port is configured as an untrusted port, then it should also be configured as an untrusted port for DHCP Snooping, or the

IP-address-MAC-address binding for this port should be configured statically. Otherwise, hosts that are attached to this port cannot respond to ARPs.

Example

The following example enables ARP inspection on the device.

```
switchxxxxxx(config)# ip arp inspection
```

11.20. ip arp inspection vlan

Use the `ip arp inspection vlan` Global Configuration mode command to enable ARP inspection on a VLAN, based on the DHCP Snooping database. Use the no form of this command to disable ARP inspection on a VLAN.

Syntax

- ip arp inspection vlan vlan-id
- no ip arp inspection vlan vlan-id

Parameters

- vlan-id - Specifies the VLAN ID.

Default Configuration

DHCP Snooping based ARP inspection on a VLAN is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables ARP inspection on a VLAN based on the DHCP snooping database. Use the `ip arp inspection list assign` command to enable static ARP inspection.

Example

The following example enables DHCP Snooping based ARP inspection on VLAN 23.

```
switchxxxxxx(config)# ip arp inspection vlan 23
```

11.21. ip arp inspection trust

Use the `ip arp inspection trust` Interface Configuration (Ethernet, Port-channel) mode command to configure an interface trust state that determines if incoming Address Resolution Protocol (ARP) packets are inspected. Use the no form of this command to restore the default configuration.

Syntax

- ip arp inspection trust
- no ip arp inspection trust

Parameters

N/A

Default Configuration

The interface is untrusted.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The device does not check ARP packets that are received on the trusted interface; it only forwards the packets.

For untrusted interfaces, the device intercepts all ARP requests and responses. It verifies that the intercepted packets have valid IP-to-MAC address bindings before updating the local cache and before forwarding the packet to the appropriate destination. The device drops invalid packets and logs them in the log buffer according to the logging configuration specified with the `ip arp inspection logging interval` command.

Example

The following example configures `te1/0/3` as a trusted interface.

```
switchxxxxxx(config)# interface te1/0/3
switchxxxxxx(config-if)# ip arp inspection trust
```

11.22. ip arp inspection validate

Use the `ip arp inspection validate` Global Configuration mode command to perform specific checks for dynamic Address Resolution Protocol (ARP) inspection. Use the no form of this command to restore the default configuration.

Syntax

- ip arp inspection validate
- no ip arp inspection validate N/A

Default Configuration

ARP inspection validation is disabled.

Command Mode

Global Configuration mode

User Guidelines

The following checks are performed:

- Source MAC address: Compares 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.
- Destination MAC address: Compares the destination MAC address in the Ethernet header against the target MAC address in the ARP body. This check is performed for ARP responses.
- IP addresses: Compares the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

Example

The following example executes ARP inspection validation.

```
switchxxxxxx(config)# ip arp inspection validate
```

11.23. ip arp inspection list create

Use the `ip arp inspection list create` Global Configuration mode command to create a static ARP binding list and enters the ARP list configuration mode. Use the no form of this command to delete the list.

Syntax

- ip arp inspection list create name
- no ip arp inspection list create name

Parameters

- name - Specifies the static ARP binding list name. (Length: 1–32 characters).

Default Configuration

No static ARP binding list exists.

Command Mode

Global Configuration mode

User Guidelines

Use the `ip arp inspection list assign` command to assign the list to a VLAN.

Example

The following example creates the static ARP binding list 'servers' and enters the ARP list configuration mode.

```
switchxxxxxx(config)# ip arp inspection list create servers
```

11.24. ip mac

Use the `ip mac` ARP-list Configuration mode command to create a static ARP binding. Use the no form of this command to delete a static ARP binding.

Syntax

- ip ip-address mac mac-address
- no ip ip-address mac mac-address

Parameters

- ip-address - Specifies the IP address to be entered to the list.
- mac-address - Specifies the MAC address associated with the IP address.

Default Configuration

No static ARP binding is defined.

Command Mode

ARP-list Configuration mode

Example

The following example creates a static ARP binding.

```
switchxxxxxx(config)# ip arp inspection list create servers
switchxxxxxx(config-arp-list)# ip 172.16.1.1 mac 0060.704C.7321
switchxxxxxx(config-arp-list)# ip 172.16.1.2 mac 0060.704C.7322
```

11.25. ip arp inspection list assign

Use the `ip arp inspection list assign` Global Configuration mode command to assign a static ARP binding list to a VLAN. Use the no form of this command to delete the assignment.

Syntax

- ip arp inspection list assign vlan-id name
- no ip arp inspection list assign vlan-id

Parameters

- vlan-id - Specifies the VLAN ID.
- name - Specifies the static ARP binding list name.

Default Configuration

No static ARP binding list assignment exists.

Command Mode

Global Configuration mode

Example

The following example assigns the static ARP binding list Servers to VLAN 37.

```
switchxxxxxx(config)# ip arp inspection list assign
37 servers
```

11.26. ip arp inspection logging interval

Use the `ip arp inspection logging interval` Global Configuration mode command to set the minimum time interval between successive ARP SYSLOG messages. Use the no form of this command to restore the default configuration.

Syntax

- ip arp inspection logging interval {seconds | infinite}
- no ip arp inspection logging interval

Parameters

- seconds - Specifies the minimum time interval between successive ARP SYSLOG messages. A 0 value means that a system message is immediately generated. (Range: 0–86400)
- infinite - Specifies that SYSLOG messages are not generated.

Default Configuration

The default minimum ARP SYSLOG message logging time interval is 5 seconds.

Command Mode

Global Configuration mode

Example

The following example sets the minimum ARP SYSLOG message logging time interval to 60 seconds.

```
switchxxxxxx(config)# ip arp inspection logging interval 60
```

11.27. show ip arp inspection

Use the `show ip arp inspection` EXEC mode command to display the ARP inspection configuration for all interfaces or for a specific interface.

Syntax

- show ip arp inspection [interface-id]

Parameters

- interface-id - Specifies an interface ID. The interface ID can be one of the following types:
  - Ethernet port
  - Port-channel.

Command Mode

User EXEC mode

Example

The following example displays the ARP inspection configuration.

```
switchxxxxxx# show ip arp inspection
IP ARP inspection is Enabled
IP ARP inspection is configured on following VLANs: 1
Verification of packet header is Enabled
IP ARP inspection logging interval is: 222 seconds
 Interface Trusted
---------- ----------
te1/0/1 Yes
te1/0/2 Yes
```

11.28. show ip arp inspection list

Use the `show ip arp inspection list` Privileged EXEC mode command to display the static ARP binding list.

Syntax

- show ip arp inspection list

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays the static ARP binding list.

```
switchxxxxxx# show ip arp inspection list
List name: servers
Assigned to VLANs: 1,2
IP    ARP
---------- --------------
172.16.0060.704C.7322
172.16.0060.704C.7322
```

11.29. show ip arp inspection statistics

Use the `show ip arp inspection statistics` EXEC command to display statistics for the following types of packets that have been processed by this feature: Forwarded, Dropped, IP/MAC Validation Failure.

Syntax

- show ip arp inspection statistics [vlan vlan-id]

Parameters

- vlan-id - Specifies VLAN ID.

Command Mode

User EXEC mode

User Guidelines

To clear ARP Inspection counters use the `clear ip arp inspection statistics` command. Counters values are kept when disabling the ARP Inspection feature.

Example

```
switchxxxxxx# show ip arp inspection statistics
Vlan Forwarded Packets Dropped Packets IP/MAC Failures
----  ---------------------------------------------
2     1500100     80
```

11.30. clear ip arp inspection statistics

Use the `clear ip arp inspection statistics` Privileged EXEC mode command to clear statistics ARP Inspection statistics globally.

Syntax

- clear ip arp inspection statistics [vlan vlan-id]

Parameters

- vlan-id - Specifies VLAN ID.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# clear ip arp inspection statistics
```

12. DHCPv6 Commands

12.1. clear ipv6 dhcp client

To restart DHCP for an IPv6 client on an interface, use the `clear ipv6 dhcp client` command in Privileged EXEC mode.

Syntax

- clear ipv6 dhcp client interface-id

Parameters

- interface-id - Interface identifier.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

This command restarts DHCP for an IPv6 client on a specified interface after first releasing and unconfiguring previously-acquired prefixes and other configuration options (for example, Domain Name System [DNS] servers).

Example

The following example restarts the DHCP for IPv6 client on VLAN 100:

```
switchxxxxxx# clear ipv6 dhcp client vlan 100
```

12.2. ipv6 address dhcp

To enable DHCP for an IPv6 client process and acquire an IPv6 address on an interface, use the `ipv6 address dhcp` command in Interface Configuration mode. To remove the address from the interface, use the no form of this command.

Syntax

- ipv6 address dhcp [rapid-commit]
- no ipv6 address dhcp

Parameters

- rapid-commit - Allows the two-message exchange method for address assignment.

Default Configuration

No IPv6 addresses are acquired from the DHCPv6 server.

Command Mode

Interface (VLAN) Configuration mode

Interface (Ethernet, Port Channel, OOB) Configuration mode

User Guidelines

This command enables IPv6 on an interface (if it is not enabled) and starts the DHCP for IPv6 client process, if this process is not yet running and if an IPv6 interface is enabled on the

interface. This command allows an interface to dynamically learn its IPv6 address by using DHCPv6 and enables the DHCPv6 Stateless service.

The rapid-commit keyword enables the use of the two-message exchange for address allocation and other configuration. If it is enabled, the client includes the rapid-commit option in a solicit message.

This command allows an interface to dynamically learn its IPv6 address by using DHCPv6.

The DHCPv6 stateless service allows to receive the configuration from a DHCP server, passed in the following options:

- Option 7: OPTION_PREFERENCE - The preference value for the server in this message
- Option 12: OPTION_UNICAST - The IP address to which the client should send messages delivered using unicast
- Option 23: OPTION_DNS_SERVERS - List of DNS Servers IPv6 Addresses
- Option 24: OPTION_DOMAIN_LIST - Domain Search List
- Option 31: OPTION_SNTP_SERVERS - List of SNTP Servers IPv6 Addresses Option 32: OPTION_INFORMATION_REFRESH_TIME - Information Refresh Time Option
- Option 41: OPTION_NEW_POSIX_TIMEZONE - New Timezone Posix String
- Option 59: OPT_BOOTFILE_URL - Configuration Server URL
- Option 60: OPT_BOOTFILE_PARAM, the first parameter - Configuration File Path Name

The DHCPv6 client uses the following IAID format based on the interface-id on which it is running:

- Octet 1, bits 7-4: These bits are reserved and must be 0
- Octet 1, Bits 3-0: These bits contain the interface type:
  - 0 - VLAN
  - 1 - Ethernet port
  - 2 - Port channel
  - 3 - Tunnel
- Octets 2-4: The octets contain a value depending on the interface type in the network format:
-
- VLAN
  - Octet 2: Reserved, must be 0
  - Octets 3-4: VLAN ID (1-4095)
- Ethernet port
  - Octet 2, bits 7-4: Slot number
  - Octet 2, bits 3-0: Port Type:
  -
  - 0 - Ethernet
  - 1 - Fast Ethernet
  - 2 - Giga Ethernet
  - 3 - 2.5Giga Ethernet
  - 4 - 5Giga Ethernet
  - 5 - 10Giga Ethernet
  - 6 - 12Giga Ethernet
  - 7 - 13.6Giga Ethernet
  - 8 - 16Giga Ethernet
  - 9 - 20Giga Ethernet
  - 10 - 40Giga Ethernet

  - 11 - 100Giga Ethernet Octet 3: Unit number
  - Octet 4: Port number
- Port channel
  - Octets 2-3: Reserved, must be 0
  - Octet 4: Port channel number
- Tunnel
  - Octets 2-3: Reserved, must be 0
  - Octet 4: Tunnel number

When IPv6 Forwarding is enabled only stateless information is required from a DHCPv6 server.

When IPv6 forwarding is changed from disabled to enabled, IPv6 addresses assigned by a DHCPv6 are removed.

When IPv6 forwarding is changed from enabled to disabled receiving IPv6 addresses from a DHCPv6 server is resumed.

The DHCPv6 client, server, and relay functions are mutually exclusive on an interface.

Example

The following example enables IPv6 on VLAN 100 and acquires an IPv6 address:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 address dhcp
switchxxxxxx(config-if)# exit
```

12.3. ipv6 dhcp client information refresh

To configure the refresh time for IPv6 client information refresh time on a specified interface if the DHCPv6 server reply does not include the Information Refresh Time, use the ip`v6 dhcp client information refresh` command in Interface Configuration mode. To return to the default value of the refresh time, use the no form of this command.

Syntax

- ipv6 dhcp client information refresh seconds | infinite
- no ipv6 dhcp client information refresh

Parameters

- seconds - The refresh time, in seconds. The value cannot be less than the minimal acceptable refresh time configured by the ipv6 dhcp client information refresh command. The maximum value that can be used is 4,294967,294 seconds (0xFFFFFFFE).
- infinite - Infinite refresh time.

Default Configuration

The default is 86,400 seconds (24 hours).

Command Mode

Interface Configuration mode

User Guidelines

The ipv6 dhcp client information refresh command specifies the information refresh time. If the server does not sends an information refresh time option then a value configured by the command is used.

Use the infinite keyword, to prevent refresh, if the server does not send an information refresh time option.

Example

The following example configures an upper limit of 2 days:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp client information refresh 172800
switchxxxxxx(config-if)# exit
```

12.4. ipv6 dhcp client information refresh minimum

To configure the minimum acceptable refresh time on the specified interface, use the `ipv6 dhcp client information refresh minimum` command in Interface Configuration mode. To remove the configured refresh time, use the no form of this command.

Syntax

- ipv6 dhcp client information refresh minimum seconds | infinite
- no ipv6 dhcp client information refresh minimum

Parameters

- seconds - The refresh time, in seconds. The minimum value that can be used is 600 seconds. The maximum value that can be used is 4,294,967,294 seconds (0xFFFFFFFE).
- infinite - Infinite refresh time.

Default Configuration

The default is 86,400 seconds (24 hours).

Command Mode

Interface Configuration mode

User Guidelines

The ipv6 dhcp client information refresh minimum command specifies the minimum acceptable information refresh time. If the server sends an information refresh time option of less than the configured minimum refresh time, the configured minimum refresh time will be used instead.

This command may be configured in the following situations:

- In unstable environments where unexpected changes are likely to occur.
- For planned changes, including renumbering. An administrator can gradually decrease the time as the planned event nears.
- Limit the amount of time before new services or servers are available to the client, such as the addition of a new Simple Network Time Protocol (SNTP) server or a change of address of a Domain Name System (DNS) server.

If you configure the infinite keyword client never refreshes the information.

Example

The following example configures an upper limit of 2 days:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp client information refresh 172800
switchxxxxxx(config-if)# exit
```

12.5. ipv6 dhcp duid-en

To set the Vendor Based on Enterprise Number DHVPv6 Unique Identified (DUID-EN) format, use the `ipv6 dhcp duid-en` command in Global Configuration mode.

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

Syntax

- ipv6 dhcp duid-en enterprise-number identifier
- no ipv6 dhcp duid-en

Parameters

- enterprise-number - The vendor's registered Private Enterprise number as maintained by IANA.
- identifier - The vendor-defined non-empty hex string (up to 64 hex characters). If the number of the character is not even '0' is added at the right. Each 2 hex characters can be separated by a period or colon.

Default Configuration

DUID Based on Link-layer Address (DUID-LL) is used. The base MAC Address is used as a Link-layer Address.

Command Mode

Global Configuration mode

User Guidelines

By default, the DHCPv6 uses the DUID Based on Link-layer Address (see RFC3315) with the Base MAC Address as a Link-layer Address.

Use this command to change the DUID format to the Vendor Based on Enterprise Number.

Examples

Example 1. The following sets the DIID-EN format:

```
ipv6 dhcp duid-en 9 0CC084D303000912
```

Example 2. The following sets the DIID-EN format using colons as delimiter:

```
switchxxxxxx(config)# ipv6 dhcp duid-en 9 0C:C0:84:D3:03:00:09:12
```

12.6. ipv6 dhcp relay destination (Global)

To specify a globally-defined relay destination address to which client messages are forwarded, use the `ipv6 dhcp relay destination` command in Global Configuration mode. To remove a relay destination address, use the no form of this command.

Syntax

- ipv6 dhcp relay destination {ipv6-address [interface-id]} | interface-id

- no ipv6 dhcp relay destination [{ipv6-address [interface-id]} | interface-id]

Parameters

- ipv6-address [interface-id] - Relay destination IPv6 address in the form documented in RFC 4291 where the address is specified in hexadecimal using 16-bit values between colons. There are the following types of relay destination address:
  - Link-local Unicast address. A user must specify the interface-id argument for this kind of address.
  - Global Unicast IPv6 address. If the interface-id argument is omitted then the Routing table is used.
- interface-id - Interface identifier that specifies the output interface for a destination. If this argument is configured, client messages are forwarded to the well-known link-local Multicast address

All_DHCP_Relay_Agents_and_Servers (FF02::1:2) through the link to which the output interface is connected.

Default Configuration

There is no globally-defined relay destination.

Command Mode

Global Configuration mode

User Guidelines

The ipv6 dhcp relay destination command specifies a destination address to which client messages are forwarded. The address is used by all DHCPv6 relays running on the switch. Up to 100 addresses can be defined.

When a relay service is running on an interface, a DHCP for IPv6 message received on that interface will be forwarded to all configured relay destinations configured per interface and globally.

Multiple destinations can be configured on one interface, and multiple output interfaces can be configured for one destination.

Unspecified, loopback, and Multicast addresses are not acceptable as the relay destination.

Use the no form of the command with the ipv6-address and interface-id arguments to remove only the given globally-defined address with the given output interface.

Use the no form of the command with the ipv6-address argument to remove only the given globally-defined address for all output interfaces.

The no form of the command without the arguments removes all the globally-defined addresses.

Examples

Example 1. The following example sets the relay unicast link-local destination address per VLAN 200:

```
switchxxxxxx(config)# ipv6 dhcp relay destination FE80::1:2 vlan 200
```

Example 2. The following example sets that client messages are forwarded to VLAN 200:

```
switchxxxxxx(config)# ipv6 dhcp relay destination vlan 200
```

Example 3. The following example sets the unicast global relay destination address:

```
switchxxxxxx(config)# ipv6 dhcp relay destination 3002::1:2
```

12.7. ipv6 dhcp relay destination (Interface)

To specify a destination address to which client messages are forwarded and to enable DHCP for IPv6 relay service on the interface, use the `ipv6 dhcp relay destination` command in Interface Configuration mode. To remove a relay destination on the interface or to delete an output interface for a destination, use the no form of this command.

Syntax

- ipv6 dhcp relay destination [{ipv6-address [interface-id]} | interface-id]
- no ipv6 dhcp relay destination [{ipv6-address [interface-id]} | interface-id]

Parameters

- ipv6-address [interface-id] - Relay destination IPv6 address in the form documented in RFC 4291 where the address is specified in hexadecimal using 16-bit values between colons. There are the following types of relay destination address:
  - Link-local Unicast address. A user must specify the interface-id argument for this kind of address.
  - Global Unicast IPv6 address. If the interface-id argument is omitted then the Routing table is used.
- interface-id - Interface identifier that specifies the output interface for a destination. If this argument is configured, client messages are forwarded to the well-known link-local Multicast address

All_DHCP_Relay_Agents_and_Servers (FF02::1:2) through the link to which the output interface is connected.

Default Configuration

The relay function is disabled, and there is no relay destination on an interface.

Command Mode

Interface Configuration mode

User Guidelines

This command specifies a destination address to which client messages are forwarded, and it enables DHCP for IPv6 relay service on the interface. Up to 10 addresses can be defined per one interface and up to 100 addresses can be defined per switch.

DHCPv6 Relay inserts the Interface-id option if an IPv6 global address is not defined on the interface on which the relay is running. The Interface-id field of the option is the interface name (a value of the ifName field of the ifTable) on which the relay is running.

When relay service is running on an interface, a DHCP for IPv6 message received on that interface will be forwarded to all configured relay destinations configured per interface and globally.

The incoming DHCP for IPv6 message may have come from a client on that interface, or it may have been relayed by another relay agent.

The relay destination can be a Unicast address of a server or another relay agent, or it may be a Multicast address. There are two types of relay destination addresses:

- A link-local Unicast or Multicast IPv6 address, for which a user must specify an output interface.
- A global Unicast IPv6 address. A user can optionally specify an output interface for this kind of address.

If no output interface is configured for a destination, the output interface is determined by routing tables. In this case, it is recommended that a Unicast or Multicast routing protocol be running on the router.

Multiple destinations can be configured on one interface, and multiple output interfaces can be configured for one destination. When the relay agent relays messages to a Multicast address, it sets the hop limit field in the IPv6 packet header to 32.

Unspecified, loopback, and node-local Multicast addresses are not acceptable as the relay destination.

Note that it is not necessary to enable the relay function on an interface for it to accept and forward an incoming relay reply message from servers. By default, the relay function is disabled, and there is no relay destination on an interface.

Use the no form of the command with arguments to remove a specific address.

Use the no form of the command without arguments to remove all the defined addresses and to disable the relay on the interface.

Examples

Example 1. The following example sets the relay Unicast link-local destination address per VLAN 200 and enables the DHCPv6 Relay on VLAN 100 if it was not enabled:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp relay destination FE80::1:2 vlan 200
switchxxxxxx(config-if)# exit
```

Example 2. The following example sets the relay well known Multicast link-local destination address per VLAN 200 and enables the DHCPv6 Relay on VLAN 100 if it was not enabled:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp relay destination vlan 200
switchxxxxxx(config-if)# exit
```

Example 3. The following example sets the Unicast global relay destination address and enables the DHCPv6 Relay on VLAN 100 if it was not enabled:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp relay destination 3002::1:2
switchxxxxxx(config-if)# exit
```

Example 4. The following example enables DHCPv6 relay on VLAN 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp relay destination
switchxxxxxx(config-if)# exit
```

Example 5. The following example disables DHCPv6 relay on VLAN 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# no ipv6 dhcp relay destination
switchxxxxxx(config-if)# exit
```

12.8. show ipv6 dhcp

To display the Dynamic DHCP unique identifier (DUID) on a specified device, use the `show ipv6 dhcp` command in User EXEC mode.This information is relevant for DHCPv6 clients and DHCPv6 relays.

Syntax

- show ipv6 dhcp

Parameters

NA

Command Mode

User EXEC mode

User Guidelines

This command uses the DUID, which is based on the link-layer address for both client and server identifiers. The device uses the MAC address from the lowest-numbered interface to form the DUID.

Examples

Example 1. The following is sample output from this command when the switch’s DUID format is vendor based on enterprise number:

```
switchxxxxxx# show ipv6 dhcp
The switch’s DHCPv6 unique identifier(DUID)is 0002000000090CC084D303000912
 Format: 2
 Enterprise Number: 9
 Identifier: 0CC084D303000912
```

Example 2. The following is sample output from this command when the switch’s DUID format is the vendor-based on link-layer address:

```
switchxxxxxx# show ipv6 dhcp
The switch’s DHCPv6 unique identifier(DUID)is 0003000100240126 07AA
 Format: 3
 Hardware type: 1
 MAC Address: 0024.0126.07AA
```

Example 3. The following is sample output from this command when the switch’s DUID format is vendorbased on link-layer address and DHCPv6 Relay is supported:

```
switchxxxxxx# show ipv6 dhcp
The switch’s DHCPv6 unique identifier(DUID)is 0003000100240126 07AA
 Format: 3
 Hardware type: 1
 MAC Address: 0024.0126.07AA
Relay Destinations:
 2001:001:250:A2FF:FEBF:A056
 2001:1001:250:A2FF:FEBF:A056
 2001:1011:250:A2FF:FEBF:A056 via VLAN 100
 FE80::250:A2FF:FEBF:A056 via VLAN 100
 FE80::250:A2FF:FEBF:A056 via VLAN 200
```

12.9. show ipv6 dhcp interface

To display DHCP for IPv6 interface information, use the `show ipv6 dhcp interface` command in User EXEC mode.

Syntax

- show ipv6 dhcp interface [interface-id]

Parameters

- interface-id - Interface identifier.

Command Mode

User EXEC mode

User Guidelines

If no interfaces are specified in the command, all interfaces on which DHCP for IPv6 (client or server) is enabled are displayed. If an interface is specified in the command, only information about the specified interface is displayed.

Note. This new output format is supported starting with the SW version supporting statefull configuration

Example

The following is sample output from this command when DHCPv6 client is enabled:

```
switchxxxxxx# show ipv6 dhcp interface
VLAN 100 is in client mode
 Configuration:
 Statefull Service is enabled (rapid-commit)
 Auto-Configuration is enabled
 Information Refresh Time: 86400 seconds Information Refresh Minimum Time: 600
seconds
 State:
 DHCP Operational mode is enabled
 Statefull Service is available DHCP server:
 Address: FE80::204:FCFF:FEA1:7439
 DUID: 000300010002FCA17400
 Preference: 20
 IPv6 Address Information:
 IA NA: IA ID 0x00040001, T1 120, T2 192 IPv6 Address: 30e0::12:45:11 preferred
lifetime: 300, valid lifetime: 54333 expires at Nov 08 2002 09:11 (54331
seconds) renew for address will be sent in 54301 seconds IPv6 Address:
3012::13:af:25 preferred lifetime: 280, valid lifetime: 51111 expires at Nov 08
2002 08:17 (51109 seconds) renew for address will be sent in 5101 seconds
 Stateless Information:
 Information Refresh Time: 86400 seconds expires at Nov 08 2002 08:17 (51109
seconds) DNS Servers: 1001::1, 2001::10
 DNS Domain Search List: company.com beta.org
 SNTP Servers: 2004::1
 POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
 Configuration Server: config.company.com
 Configuration Path Name: qqq/config/aaa_config.dat
 Indirect Image Path Name: qqq/config/aaa_image_name.txt
VLAN 105 is in client mode
 Configuration:
 Statefull Service is enabled
```

```
 Auto-Configuration is disabled
 Information Refresh Time: 86400 seconds Information Refresh Minimum Time: 600
seconds
 State:
 DHCP Operational mode is enabled
 Statefull Service is not available (IPv6 routing is enabled)
 DHCP server:
 Address: FE80::204:FCFF:FEA1:7439
 DUID: 000300010002FCA17400
 Preference: 20 Stateless Information:
 Information Refresh Time: 86400 seconds expires at Nov 08 2002 08:17 (51109
seconds)
 DNS Servers: 1001::1, 2001::10
 DNS Domain Search List: company.com beta.org
 SNTP Servers: 2004::1
 POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
 Configuration Server: config.company.com
 Configuration Path Name: qqq/config/aaa_config.dat
 Indirect Image Path Name: qqq/config/aaa_image_name.txt
VLAN 107 is in client mode
 Configuration:
 Statefull Service is enabled
 Auto-Configuration is enabled
 Information Refresh Time: 86400 seconds Information Refresh Minimum Time: 600
seconds
 State:
 DHCP Operational mode is enabled
 Statefull Service is not available (IPv6 routing is enabled)
 DHCP server:
 Address: FE80::204:FCFF:FEA1:7439
 DUID: 000300010002FCA17400
 Preference: 20 Stateless Information:
 Information Refresh Time: 86400 seconds expires at Nov 08 2002 08:17 (51109
seconds) DNS Servers: 1001::1, 2001::10
 DNS Domain Search List: company.com beta.org
 SNTP Servers: 2004::1
 POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
 Configuration Server: config.company.com
 Configuration Path Name: qqq/config/aaa_config.dat
 Indirect Image Path Name: qqq/config/aaa_image_name.txt
VLAN 110 is in client mode
 Configuration:
 Statefull Service is enabled
 Auto-Configuration is disabled
 Information Refresh Time: 86400 seconds Information Refresh Minimum Time: 600
seconds
 State:
 DHCP Operational mode is disabled (IPv6 is not enabled)
VLAN 1000 is in client mode
 Configuration:
 Statefull Service is enabled
 Auto-Configuration is enabled
 Information Refresh Time: 86400 seconds Information Refresh Minimum Time: 600
seconds
 State:
 DHCP Operational mode is disabled (Interface status is DOWN)
```

```
 DHCP server:
 Address: FE80::204:FCFF:FEA1:7439
 DUID: 000300010002FCA17400
 Preference: 20 Stateless Information:
 Information Refresh Time: 86400 seconds expires at Nov 08 2002 08:17 (51109
seconds)
 DNS Servers: 1001::1, 2001::10
 DNS Domain Search List: company.com beta.org
 SNTP Servers: 2004::1
 POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
 Configuration Server: config.company.com
 Configuration Path Name: qqq/config/aaa_config.dat
 Indirect Image Path Name: qqq/config/aaa_image_name.txt
VLAN 1010 is in relay mode
 DHCP Operational mode is enabled
 Relay source interface: VLAN 101 Relay destinations:
 2001:001:250:A2FF:FEBF:A056
 FE80::250:A2FF:FEBF:A056 via FastEthernet 1/0/10
```

13. DNS Client Commands

13.1. clear host

Use the `clear host` command in privileged EXEC mode to delete dynamic hostname-to-address mapping entries from the DNS client name-to-address cache.

Syntax

- clear host {hostname | *}

Parameters

- hostname - Name of the host for which hostname-to-address mappings are to be deleted from the DNS client name-to-address cache.
- * - Specifies that all the dynamic hostname-to-address mappings are to be deleted from the DNS client name-to-address cache.

Default Configuration

No hostname-to-address mapping entries are deleted from the DNS client name-to-address cache.

Command Mode

Privileged EXEC mode

User Guidelines

To remove the dynamic entry that provides mapping information for a single hostname, use the hostname argument. To remove all the dynamic entries, use the * keyword.

To define a static hostname-to-address mappings in the DNS hostname cache, use the `ip host` command.

To delete a static hostname-to-address mappings in the DNS hostname cache, use the `no ip host` command.

Example

The following example deletes all dynamic entries from the DNS client name-to-address cache.

```
switchxxxxxx# clear host *
```

13.2. ip domain lookup

Use the `ip domain lookup` command in Global Configuration mode to enable the IP Domain Naming System (DNS)-based host name-to-address translation.

To disable the DNS, use the no form of this command.

Syntax

- ip domain lookup
- no ip domain lookup

Parameters

N/A

Default Configuration

Enabled.

Command Mode

Global Configuration mode

Example

The following example enables DNS-based host name-to-address translation.

```
switchxxxxxx(config)# ip domain lookup
```

13.3. ip domain name

Use the `ip domain name` command in Global Configuration mode to define a default domain name that the switch uses to complete unqualified hostnames (names without a dotted-decimal domain name).

To delete the static defined default domain name, use the no form of this command.

Syntax

- ip domain name name
- no ip domain name

Parameters

- name - Default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name. Length: 1–158 characters. Maximum label length of each domain level is 63 characters.

Default Configuration

No default domain name is defined.

Command Mode

Global Configuration mode

User Guidelines

Define up to 64 static domain names or ip addresses.

Any IP hostname that does not contain a domain name (that is, any name without a dot) will have the dot and the default domain name appended to it before being added to the host table.

Domain names and host names are restricted to the ASCII letters A through Z (case-insensitive), the digits 0 through 9, the underscore and the hyphen. A period (.) is used to separate labels.

The maximum size of each domain level is 63 characters. The maximum name size is 158 bytes.

Example

The following example defines the default domain name as ‘www.website.com’.

```
switchxxxxxx(config)# ip domain name website.com
```

13.4. ip domain polling-interval

Use the `ip domain polling-interval` command in Global Configuration mode to specify the polling interval.

Use the no form of this command to return to the default behavior.

Syntax

- ip domain polling-interval seconds
- no ip domain polling-interval

Parameters

- seconds - Polling interval in seconds. The range is from (2*(R+1)*T) to 3600.

Default Configuration

The default value is 2 * (R+1) * T, where

- R is a value configured by the ip domain retry command.
- T is a value configured by the ip domain timeout command.

Command Mode

Global Configuration mode

User Guidelines

Some applications communicate with the given IP address continuously. DNS clients for such applications, which have not received resolution of the IP address or have not detected a DNS server using a fixed number of retransmissions, return an error to the application and continue to send DNS Request messages for the IP address using the polling interval.

Example

The following example shows how to configure the polling interval of 100 seconds:

```
switchxxxxxx(config)# ip domain polling-interval 100
```

13.5. ip domain retry

Use the `ip domain retry` command in Global Configuration mode to specify the number of times the device will send Domain Name System (DNS) queries when there is no replay.

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

Syntax

- ip domain retry number
- no ip domain retry

Parameters

- number - Number of times to retry sending a DNS query to the DNS server. The range is from 0 to 16.

Default Configuration

The default value is 1.

Command Mode

Global Configuration mode

User Guidelines

The number argument specifies how many times the DNS query will be sent to a DNS server until the switch decides that the DNS server does not exist.

Example

The following example shows how to configure the switch to send out 10 DNS queries before giving up:

```
switchxxxxxx(config)# ip domain retry 10
```

13.6. ip domain timeout

Use the `ip domain timeout` command in Global Configuration mode to specify the amount of time to wait for a response to a DNS query.

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

Syntax

- ip domain timeout seconds
- no ip domain timeout

Parameters

- seconds - Time, in seconds, to wait for a response to a DNS query. The range is from 1 to 60.

Default Configuration

The default value is 2 seconds.

Command Mode

Global Configuration mode

User Guidelines

Use the command to change the default time out value. Use the no form of this command to return to the default time out value.

Example

The following example shows how to configure the switch to wait 50 seconds for a response to a DNS query:

```
switchxxxxxx(config)# ip domain timeout 50
```

13.7. ip host

Use the `ip host` Global Configuration mode command to define the static host name-to-address mapping in the DNS host name cache.

Use the no form of this command to remove the static host name-to-address mapping.

Syntax

- ip host hostname address1 [address2...address8]
- no ip host name ip host name [address1...address8]

Parameters

- hostname - Name of the host. (Length: 1–158 characters. Maximum label length of each domain level is 63 characters).
- address1 - Associated host IP address (IPv4 or IPv6, if IPv6 stack is supported).
- address2...address8 - Up to seven additional associated IP addresses, delimited by a single space (IPv4 or IPv6, if IPv6 stack is supported).

Default Configuration

No host is defined.

Command Mode

Global Configuration mode

User Guidelines

Host names are restricted to the ASCII letters A through Z (case-insensitive), the digits 0 through 9, the underscore and the hyphen. A period (.) is used to separate labels.

An IP application will receive the IP addresses in the following order:

- IPv6 addresses in the order specified by the command.
- IPv4 addresses in the order specified by the command.

Use the no format of the command with the address1...address8 argument to delete the specified addresses. The entry is deleted if all its addresses are deleted.

Example

The following example defines a static host name-to-address mapping in the host cache.

```
switchxxxxxx(config)# ip host accounting.website.com 176.10.23.1
```

13.8. ip name-server

Use the `ip name-server` command in Global Configuration mode to specify the address of one or more name servers to use for name and address resolution.

Use the no form of this command to remove the static specified addresses.

Syntax

- ip name-server server1-address [server-address2...erver-address8]
- no ip name-server [server-address1...server-address8]

Parameters

- server-address1 - IPv4 or IPv6 addresses of a single name server.
- server-address2...server-address8 - IPv4 or IPv6 addresses of additional name servers.

Default Configuration

No name server IP addresses are defined.

Command Mode

Global Configuration mode

User Guidelines

The preference of the servers (up to 8 servers) is determined by the order in which they were entered.

Each ip name-server command replaces the configuration defined by the previous one (if one existed).

Example

The following example shows how to specify IPv4 hosts 172.16.1.111, 172.16.1.2, and IPv6 host 2001:0DB8::3 as the name servers:

```
switchxxxxxx(config)# ip name-server 172.16.1.111 172.16.1.2 2001:0DB8::3
```

13.9. show hosts

Use the `show hosts` command in privileged EXEC mode to display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.

Syntax

- show hosts [all | hostname]

Parameters

- all - The specified host name cache information is to be displayed for all configured DNS views. This is the default.
- hostname - The specified host name cache information displayed is to be limited to entries for a particular host name.

Command Mode

Privileged EXEC mode

Default Configuration

Default is all.

User Guidelines

This command displays the default domain name, a list of name server hosts, and the cached list of host names and addresses.

Example

The following is sample output with no parameters specified:

```
switchxxxxxx# show hosts
Name/address lookup is enabled
Domain Timeout: 3 seconds
Domain Retry: 4 times
Domain Polling Interval: 10 seconds
Default Domain Table
Source Interface Preference Domain static website.com dhcpv6 vlan 100 1
qqtca.com dhcpv6 vlan 100 2 company.com dhcpv6 vlan 1100 1 pptca.com
Name Server Table
Source Interface Preference IP Address static 1 192.0.2.204 static 2 192.0.2.205
static 3 192.0.2.105
DHCPv6 vlan 100 1 2002:0:22AC::11:231A:0BB4
DHCPv4 vlan 1 1 192.1.122.20 DHCPv4 vlan 1 2 154.1.122.20
Casche Table
Flags: (static/dynamic, OK/Ne/??)
OK - Okay, Ne - Negative Cache, ?? - No Response Host Flag Address;Age...in
preference order
example1.company.com (dynamic, OK) 2002:0:130F::0A0:1504:0BB4;1 112.0.2.10
176.16.8.8;123 124 173.0.2.30;39 example2.company.com (dynamic, ??)
example3.company.com (static, OK) 120.0.2.27 example4.company.com (dynamic, OK)
24 173.0.2.30;15 example5.company.com (dynamic, Ne); 12
```

14. Denial of Service (DoS) Commands

14.1. security-suite deny fragmented

To discard IP fragmented packets from a specific interface, use the `security-suite deny fragmented` Interface (Ethernet, Port Channel) Configuration mode command.

To permit IP fragmented packets, use the no form of this command.

Syntax

- security-suite deny fragmented {[add {ip-address | any} {mask | /prefix-length}] | [remove {ip-address | any} {mask | /prefix-length}]}
- no security-suite deny fragmented

Parameters

- add ip-address | any - Specifies the destination IP address. Use any to specify all IP addresses.
- mask - Specifies the network mask of the IP address.
- prefix-length - Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/).

Default Configuration

Fragmented packets are allowed from all interfaces.

If mask is unspecified, the default is 255.255.255.255.

If prefix-length is unspecified, the default is 32.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

For this command to work, `show security-suite configuration` must be enabled both globally and for interfaces.

Example

The following example attempts to discard IP fragmented packets from an interface.

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# security-suite deny fragmented add any /32
```

To perform this command, DoS Prevention must be enabled in the per-interface mode.

14.2. security-suite deny icmp

To discard ICMP echo requests from a specific interface (to prevent attackers from knowing that the device is on the network), use the `security-suite deny icmp` Interface (Ethernet, Port Channel) Configuration mode command.

To permit echo requests, use the no form of this command.

Syntax

- security-suite deny icmp {[add {ip-address | any} {mask | /prefix-length}] | [remove {ip-address | any} {mask | /prefix-length}]}

- no security-suite deny icmp

Parameters

- ip-address | any - Specifies the destination IP address. Use any to specify all IP addresses.
- mask - Specifies the network mask of the IP address.
- prefix-length - Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/).

Default Configuration

Echo requests are allowed from all interfaces.

If mask is not specified, it defaults to 255.255.255.255.

If prefix-length is not specified, it defaults to 32.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

For this command to work, `show security-suite configuration` must be enabled both globally and for interfaces.

This command discards ICMP packets with "ICMP type= Echo request" that ingress the specified interface.

Example

The following example attempts to discard echo requests from an interface.

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# security-suite deny icmp add any /32
```

To perform this command, DoS Prevention must be enabled in the per-interface mode.

14.3. security-suite deny martian-addresses

To deny packets containing system-reserved IP addresses or user-defined IP addresses, use the `security-suite deny martian-addresses` Global Configuration mode command.

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

Syntax

- security-suite deny martian-addresses {add {ip-address {mask | /prefix-length}} | remove {ip-address {mask | /prefix-length}}
  (Add/remove user-specified IP addresses)
- security-suite deny martian-addresses reserved {add | remove}
  (Add/remove system-reserved IP addresses, see tables below)
- no security-suite deny martian-addresses
  (This command removes addresses reserved by security-suite deny martian-addresses {add {ip-address {mask | /prefix-length}} | remove {ip-address {mask | /prefix-length}}, and removes all entries added by the user. The user can remove a specific entry by using remove ip-address {mask | /prefix-length} parameter.

There is no no form of the security-suite deny martian-addresses reserved {add | remove} command. Use instead the security-suite deny martian-addresses reserved remove command to remove protection (and free up hardware resources).

Parameters

- reserved add/remove - Add or remove the table of reserved addresses below.
- ip-address - Adds/discards packets with the specified IP source or destination address.
- mask - Specifies the network mask of the IP address.
- prefix-length - Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/).
- reserved - Discards packets with the source or destination IP address in the block of the reserved (Martian) IP addresses. See the User Guidelines for a list of reserved addresses.

Default Configuration

Martian addresses are allowed.

Command Mode

Global Configuration mode

User Guidelines

For this command to work, `show security-suite configuration` must be enabled globally.

`security-suite deny martian-addresses reserved` adds or removes the addresses in the following table:

Address Block	Present Use
0.0.0.0/8 (except when 0.0.0.0/32 is the source address)	Addresses in this block refer to source hosts on "this" network.
127.0.0.0/8	This block is assigned for use as the Internet host loopback address.
192.0.2.0/24	This block is assigned as "TEST-NET" for use in documentation and example code.
224.0.0.0/4 as source	This block, formerly known as the Class D address space, is allocated for use in IPv4 multicast address assignments.
240.0.0.0/4 (except when 255.255.255.255/32 is the destination address)	This block, formerly known as the Class E address space, is reserved.

Note:
If the reserved addresses are included, individual reserved addresses cannot be removed.

Example

The following example discards all packets with a source or destination address in the block of the reserved IP addresses.

```
switchxxxxxx(config)# security-suite deny martian-addresses reserved add
```

14.4. security-suite deny syn

To block the creation of TCP connections from a specific interface, use the `security-suite deny syn` Interface (Ethernet, Port Channel) Configuration mode command. This a complete block of these connections.

To permit creation of TCP connections, use the no form of this command.

Syntax

- security-suite deny syn {[add {tcp-port | any} {ip-address | any} {mask | /prefix-length}] | [remove {tcp-port | any} {ip-address | any} {mask | /prefix-length}]}
- no security-suite deny syn

Parameters

- ip-address | any - Specifies the destination IP address. Use any to specify all IP addresses.
- mask - Specifies the network mask of the destination IP address.
- prefix-length - Specifies the number of bits that comprise the destination IP address prefix. The prefix length must be preceded by a forward slash (/).
- tcp-port | any - Specifies the destination TCP port. The possible values are:
  - http,
  - ftp-control,
  - ftp-data,
  - ssh,
  - telnet,
  - smtp,
  - port number.
  -
  - Use any to specify all ports.

Default Configuration

Creation of TCP connections is allowed from all interfaces.

If the mask is not specified, it defaults to 255.255.255.255.

If the prefix-length is not specified, it defaults to 32.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

For this command to work, `show security-suite configuration` must be enabled both globally and for interfaces.

The blocking of TCP connection creation from an interface is done by discarding ingress TCP packets with "SYN=1", "ACK=0" and "FIN=0" for the specified destination IP addresses and destination TCP ports.

Example

The following example attempts to block the creation of TCP connections from an interface. It fails because security suite is enabled globally and not per interface.

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# security-suite deny syn add any /32 any
```

To perform this command, DoS Prevention must be enabled in the per-interface mode.

14.5. security-suite deny syn-fin

To drop all ingressing TCP packets in which both SYN and FIN are set, use the `security-suite deny syn-fin` Global Configuration mode command.

To permit TCP packets in which both SYN and FIN are set, use the no form of this command.

Syntax

- security-suite deny syn-fin
- no security-suite deny syn-fin

Parameters

This command has no arguments or keywords.

Default Configuration

The feature is disabled by default.

Command Mode

Global Configuration mode

Example

The following example blocks TCP packets in which both SYN and FIN flags are set.

```
switchxxxxxx(config)# security-suite deny sin-fin
```

14.6. security-suite dos protect

To protect the system from specific well-known Denial of Service (DoS) attacks, use the `security-suite dos protect` Global Configuration mode command. There are three types of attacks against which protection can be supplied (see parameters below).

To disable DoS protection, use the no form of this command.

Syntax

- security-suite dos protect {add attack | remove attack}
- no security-suite dos protect

Parameters

- add/remove attack - Specifies the attack type to add/remove. To add an attack is to provide protection against it; to remove the attack is to remove protection. The possible attack types are:
  - stacheldraht - Discards TCP packets with source TCP port 16660.
  - invasor-trojan - Discards TCP packets with destination TCP port 2140 and source TCP port 1024.

- back-orifice-trojan - Discards UDP packets with destination UDP port 31337 and source UDP port 1024.

Default Configuration

No protection is configured.

Command Mode

Global Configuration mode

User Guidelines

For this command to work, `show security-suite configuration` must be enabled globally.

Example

The following example protects the system from the Invasor Trojan DOS attack.

```
switchxxxxxx(config)# security-suite dos protect add invasor-trojan
```

14.7. security-suite dos syn-attack

To rate limit Denial of Service (DoS) SYN attacks, use the `security-suite dos syn-attack` Interface Configuration mode command. This provides partial blocking of SNY packets (up to the rate that the user specifies).

To disable rate limiting, use the no form of this command.

Syntax

- security-suite dos syn-attack syn-rate {any | ip-address} {mask | prefix-length}
- no security-suite dos syn-attack {any | ip-address} {mask | prefix-length}

Parameters

- syn-rate - Specifies the maximum number of connections per second. (Range: 199–1000)
- any | ip-address - Specifies the destination IP address. Use any to specify all IP addresses.
- mask - Specifies the network mask of the destination IP address.
- prefix-length - Specifies the number of bits that comprise the destination IP address prefix. The prefix length must be preceded by a forward slash (/).

Default Configuration

No rate limit is configured.

If ip-address is unspecified, the default is 255.255.255.255 If prefix-length is unspecified, the default is 32.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

For this command to work, `show security-suite configuration` must be enabled both globally and for interfaces.

This command rate limits ingress TCP packets with "SYN=1", "ACK=0" and "FIN=0" for the specified destination IP addresses.

SYN attack rate limiting is implemented after the security suite rules are applied to the packets. The ACL and QoS rules are not applied to those packets.

Since the hardware rate limiting counts bytes, it is assumed that the size of "SYN" packets is short.

Example

The following example attempts to rate limit DoS SYN attacks on a port. It fails because security suite is enabled globally and not per interface.

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# security-suite dos syn-attack 199 any /10
```

To perform this command, DoS Prevention must be enabled in the per-interface mode.

14.8. security-suite enable

To enable the security suite feature, use the `security-suite enable` Global Configuration mode command. This feature supports protection against various types of attacks.

When this command is used, hardware resources are reserved. These hardware resources are released when the no security-suite enable command is entered.

The security-suite feature can be enabled in one of the following ways:

- Global-rules-only - This enables the feature globally but per-interface features are not enabled.
- All (no keyword) - The feature is enabled globally and per-interface.

To disable the security suite feature, use the no form of this command.

When security-suite is enabled, you can specify the types of protection required. The following commands can be used:

- `show security-suite configuration`
- `show security-suite configuration`
- `show security-suite configuration`
- `show security-suite configuration`
- `show security-suite configuration`
- `show security-suite configuration`
- `show security-suite configuration`
- `show security-suite configuration`

Syntax

- security-suite enable [global-rules-only]
- no security-suite enable

Parameters

- global-rules-only - (Optional) Specifies that all the security suite commands are global commands only (they cannot be applied per-interface). This setting saves space in the Ternary Content Addressable Memory (TCAM). If this keyword is not used, security-suite commands can be used both globally on per-interface.

Default Configuration

The security suite feature is disabled.

If global-rules-only is not specified, the default is to enable security-suite globally and per interfaces.

Command Mode

Global Configuration mode

User Guidelines

MAC ACLs must be removed before the security-suite is enabled. The rules can be re-entered after the security-suite is enabled.

If ACLs or policy maps are assigned on interfaces, per interface security-suite rules cannot be enabled.

Examples

Example 1 - The following example enables the security suite feature and specifies that security suite commands are global commands only. When an attempt is made to configure security-suite on a port, it fails.

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# security-suite dos syn-attack 199 any /10
```

To perform this command, DoS Prevention must be enabled in the per-interface mode.

Example 2 - The following example enables the security suite feature globally and on interfaces. The security-suite command succeeds on the port.

```
switchxxxxxx(config)# security-suite enable
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# security-suite dos syn-attack 199 any /10
switchxxxxxx(config-if)#
```

14.9. security-suite syn protection mode

To set the TCP SYN protection mode, use the `security-suite syn protection mode` Global Configuration mode command.

To set the TCP SYN protection mode to default, use the no form of this command.

Syntax

- security-suite syn protection mode {disabled | report | block}
- no security-suite syn protection mode

Parameters

- disabled - Feature is disabled
- report - Feature reports about TCP SYN traffic per port (including rate-limited SYSLOG message when an attack is identified)
- block - TCP SYN traffic from attacking ports destined to the local system is blocked, and a rate-limited SYSLOG message (one per minute) is generated

Default Configuration

The default mode is block.

Command Mode

Global Configuration mode

User Guidelines

On ports in which an ACL is defined (user-defined ACL etc.), this feature cannot block TCP SYN packets. In case the protection mode is block but SYN Traffic cannot be blocked, a relevant SYSLOG message will be created, e.g.: "port te1/0/1 is under TCP SYN attack. TCP SYN traffic cannot be blocked on this port since the port is bound to an ACL."

Examples

Example 1: The following example sets the TCP SYN protection feature to report TCP SYN attack on ports in case an attack is identified from these ports.

```
switchxxxxxx(config)# security-suite syn protection mode report
…
01-Jan-2012 05:29:46: A TCP SYN Attack was identified on port te1/0/1
```

Example 2: The following example sets the TCP SYN protection feature to block TCP SYN attack on ports in case an attack is identified from these ports.

```
switchxxxxxx(config)# security-suite syn protection mode block
…
01-Jan-2012 05:29:46: A TCP SYN Attack was identified on port te1/0/1. TCP SYN
traffic destined to the local system is automatically blocked for 100 seconds.
```

14.10. security-suite syn protection recovery

To set the time period for the SYN Protection feature to block an attacked interface, use the `security-suite syn protection recovery` Global Configuration mode command.

To set the time period to its default value, use the no form of this command.

Syntax

- security-suite syn protection recovery timeout
- no security-suite syn protection recovery

Parameters

- timeout - Defines the timeout (in seconds) by which an interface from which SYN packets are blocked gets unblocked. Note that if a SYN attack is still active on this interface it might become blocked again. (Range: 10-600)

Default Configuration

The default timeout is 60 seconds.

Command Mode

Global Configuration mode

User Guidelines

If the timeout is modified, the new value will be used only on interfaces which are not currently under attack.

Example

The following example sets the TCP SYN period to 100 seconds.

```
switchxxxxxx(config)# security-suite syn protection recovery 100
```

14.11. security-suite syn protection threshold

To set the threshold for the SYN protection feature, use the `security-suite syn protection threshold` Global Configuration mode command.

To set the threshold to its default value, use the no form of this command.

Syntax

- security-suite syn protection threshold syn-packet-rate
- no security-suite syn protection threshold

Parameters

- syn-packet-rate - defines the rate (number of packets per second) from each specific port that triggers identification of TCP SYN attack. (Range: 20-200)

Default Configuration

The default threshold is 80pps (packets per second).

Command Mode

Global Configuration mode

Example

The following example sets the TCP SYN protection threshold to 40 pps.

```
switchxxxxxx(config)# security-suite syn protection threshold 40
```

14.12. show security-suite configuration

To display the security-suite configuration, use the `show security-suite configuration` command.

Syntax

- show security-suite configuration

Command Mode

User EXEC mode

Example

The following example displays the security-suite configuration.

```
switchxxxxxx# show security-suite configuration
Security suite is enabled (Per interface rules are enabled).
Denial Of Service Protect: stacheldraht, invasor-trojan, back-office-trojan.
Denial Of Service SYN-FIN Attack is enabled
Denial Of Service SYN Attack
Interface          IP Address     SYN Rate (pps)
-----------------  -------------  --------------
te1/0/1            176.16.23.0\24 100
Martian addresses filtering
Reserved addresses: enabled.
Configured addresses: 10.0.0.0/8, 192.168.0.0/16
SYN filtering
--------------
```

```
Interface IP Address TCP port
--------------- ------------- ----------
te1/0/2 176.16.23.0\24 FTP
ICMP filtering
Interface IP Address
--------- ----------
te1/0/2 176.16.23.0\24
Fragmented packets filtering
Interface IP Address
--------- ----------
te1/0/2 176.16.23.0\24
```

14.13. show security-suite syn protection

To display the SYN Protection feature configuration and the operational status per interface-id, including the time of the last attack per interface, use the `show security-suite syn protection` command.

Syntax

- show security-suite syn protection [interface-id]

Parameters

- interface-id - (Optional) Specifies an interface-ID. The interface-ID can be one of the following types:
  - Ethernet port of Port-Channel.

Command Mode

User EXEC mode

User Guidelines

Use the Interface-ID to display information on a specific interface.

Example

The following example displays the TCP SYN protection feature configuration and current status on all interfaces. In this example, port te1/0/2 is attacked but since there is a user-ACL on this port, it cannot become blocked so its status is **Reported** and not **Blocked and Reported**.

```
switchxxxxxx# show security-suite syn protection
Protection Mode: Block
Threshold: 40 Packets Per Second
Period: 100 Seconds
Interface Name Current Status Last Attack
te1/0/1 Attacked 19:58:22.289 PDT Feb 19 2012 Blocked and Reported
te1/0/2 Attacked 19:58:22.289 PDT Feb 19 2012 Reported
te1/0/3 Attacked 19:58:22.289 PDT Feb 19 2012 Blocked and Reported
```

15. EEE Commands

15.1. eee enable (global)

To enable the EEE mode globally, use the `eee enable` Global Configuration command. To disable the mode, use the no format of the command.

Note:
EEE mode is supported on all copper ports, but not with OOB ports.

Syntax

- eee enable
- no eee enable

Parameters

This command has no arguments or keywords.

Default Configuration

EEE is enabled.

Command Mode

Global Configuration mode

User Guidelines

In order for EEE to work, the device at the other end of the link must also support EEE and have it enabled. In addition, for EEE to work properly, auto-negotaition must be enabled; however, if the port speed is negotiated as 1Giga, EEE always works regardless of whether the auto-negotiation status is enabled or disabled.

If auto-negotiation is not enabled on the port and its speed is less than 1 Giga, the EEE operational status is disabled.

Example

```
switchxxxxxx(config)# eee enable
```

15.2. eee enable (interface)

To enable the EEE mode on an Ethernet port, use the `eee enable` Interface Configuration command. To disable the mode, use the no format of the command.

Syntax

- eee enable
- no eee enable

Parameters

This command has no arguments or keywords.

Default Configuration

EEE is enabled.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

If auto-negotiation is not enabled on the port and its speed is 1 Giga, the EEE operational status is disabled.

Example

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# eee enable
```

15.3. eee lldp enable

To enable EEE support by LLDP on an Ethernet port, use the `eee lldp enable` Interface Configuration command. To disable the support, use the no format of the command.

Syntax

- eee lldp enable
- no eee lldp enable

Parameters

This command has no arguments or keywords.

Default Configuration

Enabled

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

Enabling EEE LLDP advertisement enables devices to choose and change system wake-up times in order to get the optimal energy saving mode.

Example

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# eee lldp enable
```

15.4. show eee

Use the `show eee` EXEC command to display EEE information.

Syntax

- show eee [interface-id]

Parameters

- interface-id - (Optional) Specify an Ethernet port.

Defaults

None

Command Mode

Privileged EXEC mode

User Guidelines

If the port is a 10G port, but the link speed is 1G, the EEE Remote status cannot be resolved (and displayed).

Examples

Example 1 - The following displays brief Information about all ports.

```
switchxxxxxx# show eee
EEE globally enabled
EEE Administrate status is enabled on ports: te1/0/1-2, te1/0/4
EEE Operational status is enabled on ports: te1/0/1-2, te1/0/4
EEE LLDP Administrate status is enabled on ports: te1/0/1-3
EEE LLDP Operational status is enabled on ports: te1/0/1-2
```

Example 2 - The following is the information displayed when a port is in the Not Present state; no information is displayed if the port supports EEE.

```
switchxxxxxx# show eee te1/0/1 Port Status: notPresent
EEE Administrate status: enabled
EEE LLDP Administrate status: enabled
```

Example 3 - The following is the information displayed when the port is in status DOWN.

```
switchxxxxxx# show eee te1/0/1
Port Status: DOWN
EEE capabilities:
 Speed 10M: EEE not supported
 Speed 100M: EEE supported
 Speed 1G: EEE supported
 Speed 10G: EEE not supported
EEE Administrate status: enabled
EEE LLDP Administrate status: enabled
```

Example 4 - The following is the information displayed when the port is in status UP and does not support EEE.

```
switchxxxxxx# show eee te1/0/2
Port Status: UP
EEE capabilities:
 Speed 10M: EEE not supported
 Speed 100M: EEE supported
 Speed 1G: EEE supported
 Speed 10G: EEE not supported Current port speed: 1000Mbps
EEE Administrate status: enabled
EEE LLDP Administrate status: enabled
```

Example 5 - The following is the information displayed when the neighbor does not support EEE.

```
switchxxxxxx# show eee te1/0/4
Port Status: UP
EEE capabilities:
 Speed 10M: EEE not supported
 Speed 100M: EEE supported
 Speed 1G: EEE supported
 Speed 10G: EEE not supported
Current port speed: 1000Mbps
EEE Remote status: disabled
EEE Administrate status: enabled
EEE Operational status: disabled (neighbor does not support)
EEE LLDP Administrate status: enabled
```

```
EEE LLDP Operational status: disabled
```

Example 6 - The following is the information displayed when EEE is disabled on the port.

```
switchxxxxxx# show eee te1/0/1
Port Status: UP
EEE capabilities:
 Speed 10M: EEE not supported
 Speed 100M: EEE supported
 Speed 1G: EEE supported
 Speed 10G: EEE not supported Current port speed: 1000Mbps
EEE Administrate status: disabled
EEE Operational status: disabled
EEE LLDP Administrate status: enabled
EEE LLDP Operational status: disabled
```

Example 7 - The following is the information displayed when EEE is running on the port, and EEE LLDP is disabled.

```
switchxxxxxx# show eee te1/0/2
Port Status: UP
EEE capabilities:
 Speed 10M: EEE not supported
 Speed 100M: EEE supported
 Speed 1G: EEE supported
 Speed 10G: EEE not supported Current port speed: 1000Mbps
EEE Remote status: enabled
EEE Administrate status: enabled
EEE Operational status: enabled
EEE LLDP Administrate status: disabled
EEE LLDP Operational status: disabled
Resolved Tx Timer: 10usec
Local Tx Timer: 10 usec
Resolved Timer: 25 usec
Local Rx Timer: 20 usec
```

Example 8 - The following is the information displayed when EEE and EEE LLDP are running on the port.

```
switchxxxxxx# show eee te1/0/3
Port Status: UP
EEE capabilities:
 Speed 10M: EEE not supported
 Speed 100M: EEE supported
 Speed 1G: EEE supported
 Speed 10G: EEE not supported Current port speed: 1000Mbps
EEE Remote status: enabled
EEE Administrate status: enabled
EEE Operational status: enabled
EEE LLDP Administrate status: enabled
EEE LLDP Operational status: enabled
Resolved Tx Timer: 10usec
Local Tx Timer: 10 usec
Remote Rx Timer: 5 usec
Resolved Timer: 25 usec
Local Rx Timer: 20 usec
Remote Tx Timer: 25 usec
```

Example 9 - The following is the information displayed when EEE is running on the port, EEE LLDP is enabled but not synchronized with the remote link partner.

```
switchxxxxxx# show eee te1/0/4
Port Status: up
EEE capabilities:
 Speed 10M: EEE not supported
 Speed 100M: EEE supported
 Speed 1G: EEE supported
 Speed 10G: EEE not supported Current port speed: 1000Mbps
EEE Remote status: enabled
EEE Administrate status: enabled
EEE Operational status: enabled
EEE LLDP Administrate status: enabled
EEE LLDP Operational status: disabled
Resolved Tx Timer: 64
Local Tx Timer: 64
Resolved Rx Timer: 16
Local Rx Timer: 16
```

Example 10 - The following is the information displayed when EEE and EEE LLDP are running on the port.

```
show eee te1/0/3
Port Status: UP
EEE capabilities:
 Speed 10M: EEE not supported
 Speed 100M: EEE supported
 Speed 1G: EEE supported
 Speed 10G: EEE not supported Current port speed: 1000Mbps
EEE Remote status: enabled
EEE Administrate status: enabled
EEE Operational status: enabled
EEE LLDP Administrate status: enabled
EEE LLDP Operational status: enabled
Resolved Tx Timer: 10usec
Local Tx Timer: 10 usec
Remote Rx Timer: 5 usec
Resolved Timer: 25 usec
Local Rx Timer: 20 usec
Remote Tx Timer: 25 usec
```

16. Ethernet Configuration Commands

16.1. interface

To enter Interface configuration mode in order to configure an interface, use the `interface` Global Configuration mode command.

Syntax

- interface interface-id

Parameters

- interface-id - Specifies an interface ID. The interface ID can be one of the following types:
  - Ethernet port,
  - port-channel,
  - VLAN,
  - range,
  - OOB,
  - IP interface,
  - tunnel.

Default Configuration

None

Command Mode

Global Configuration mode

Examples

Example 1 - For Ethernet ports:

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)#
```

Example 2 - For port channels (LAGs):

```
switchxxxxxx(config)# interface po1
switchxxxxxx(config-if)#
```

16.2. interface range

To execute a command on multiple ports at the same time, use the `interface range` command.

Syntax

- interface range interface-id-list

Parameters

- interface-id-list - Specify list of interface IDs. The interface ID can be one of the following types:
  - Ethernet port,
  - VLAN,
  - port-channel

Default Configuration

None

Command Mode

Interface (Ethernet, Port Channel, VLAN) Configuration mode

User Guidelines

Commands under the interface range context are executed independently on each interface in the range. If the command returns an error on one of the interfaces, it does not stop the execution of the command on other interfaces.

Example

```
switchxxxxxx(config)# interface range te1/0/1-4
switchxxxxxx(config-if-range)#
```

16.3. shutdown

To disable an interface, use the `shutdown` Interface Configuration mode command.

To restart a disabled interface, use the no form of this command.

Syntax

- shutdown
- no shutdown

Parameters

This command has no arguments or keywords.

Default Configuration

The interface is enabled.

Command Mode

Interface Configuration mode

User Guidelines

The `shutdown` command set a value of ifAdminStatus (see RFC 2863) to DOWN.

When ifAdminStatus is changed to DOWN, ifOperStatus will be also changed to DOWN.

The DOWN state of ifOperStatus means that the interface does not transmit/receive messages from/to higher levels. For example, if you shut down a VLAN, on which an IP interface is configured, bridging into the VLAN continues, but the switch cannot transmit and receive IP traffic on the VLAN.

Notes:

- If the switch shuts down an Ethernet port it additionally shuts down the port MAC sublayer too.
- If the switch shuts down a port channel it additionally shuts down all ports of the port channel too.
- The `shutdown` command recovers an Err-Disable status of a port.

Examples

Example 1 - The following example disables te1/0/`4` operations.

```
switchxxxxxx(config)# interface te1/0/4
switchxxxxxx(config-if)# shutdown
switchxxxxxx(config-if)#
```

Example 2 - The following example restarts the disabled Ethernet port.

```
switchxxxxxx(config)# interface te1/0/4
switchxxxxxx(config-if)# no shutdown
switchxxxxxx(config-if)#
```

Example 3 - The following example shuts down vlan 100.

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# shutdown
switchxxxxxx(config-if)#
```

Example 4 - The following example shuts down tunnel 1.

```
switchxxxxxx(config)# interface tunnel 1
switchxxxxxx(config-if)# shutdown
switchxxxxxx(config-if)#
```

Example 5 - The following example shuts down Port Channel 3.

```
switchxxxxxx(config)# interface po3
switchxxxxxx(config-if)# shutdown
switchxxxxxx(config-if)#
```

16.4. operation time

To control the time that the port is up, use the `operation time` Interface (Ethernet, Port Channel) Configuration mode command. To cancel the time range for the port operation time, use the no form of this command.

Syntax

- operation time time-range-name
- no operation time

Parameters

- time-range-name - Specifies a time range the port operates (in up state). When the Time Range is not in effect, the port is shutdown. (Range: 1–32 characters)

Default Configuration

There is no time range configured on the port authorized state.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

It is recommended to disable spanning tree or to enable spanning-tree PortFast mode on 802.1x edge ports (ports in auto state that are connected to end stations), in order to proceed to the forwarding state immediately after successful authentication.

Example

The operation time command influences the port if the port status is up. This command defines the time frame during which the port stays up and at which time the port will be shutdown. While the port is in shutdown because of other reasons, this command has no effect.

The following example activates an operation time range (named "morning") on port te1/0/1.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# operation time morning
```

16.5. description

To add a description to an interface, use the `description` Interface (Ethernet, Port Channel) Configuration mode command. To remove the description, use the no form of this command.

Syntax

- description string
- no description

Parameters

- string - Specifies a comment or a description of the port to assist the user. (Length: 1–64 characters).

Default Configuration

The interface does not have a description.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example adds the description 'SW#3' to te1/0/4.

```
switchxxxxxx(config)# interface te1/0/4
switchxxxxxx(config-if)# description SW#3
```

16.6. speed

To configure the speed of a given Ethernet interface when not using auto-negotiation, use the `speed` Interface (Ethernet, Port Channel) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- speed {100 | 1000 | 10000}
- no speed

Parameters

- 100 - Forces 100 Mbps operation
- 1000 - Forces 1000 Mbps operation
- 10000 - Forces 10000 Mbps operation

Default Configuration

The port operates at its maximum speed capability.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The no speed command in a port-channel context returns each port in the port-channel to its maximum capability.

Example

The following example configures the speed of te1/0/4 to 100 Mbps operation.

```
switchxxxxxx(config)# interface te1/0/4
switchxxxxxx(config-if)# speed 100
```

16.7. duplex

To configure the full/half duplex operation of a given Ethernet interface when not using auto-negotiation, use the duplex Interface (Ethernet, Port Channel) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- duplex {half | full}
- no duplex

Parameters

- half - Forces half-duplex operation.
- full - Forces full-duplex operation.

Default Configuration

The interface operates in full duplex mode.

Command Mode

Interface (Ethernet) Configuration mode

Example

The following example configures te1/0/1 to operate in full duplex mode.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# duplex full
```

16.8. negotiation

To enable auto-negotiation operation for the speed and duplex parameters and master-slave mode of a given interface, use the negotiation Interface (Ethernet, Port Channel) Configuration mode command. To disable auto-negotiation, use the no form of this command.

Syntax

- negotiation [capability [capability2... capability5]] [preferred {master | slave}]
- no negotiation

Parameters

- Capability - (Optional) Specifies the capabilities to advertise. (Possible values: 10h, 10f, 100h,100f, 1000f ,10000f).
  - 10h - Advertise 10 half-duplex

- 10f - Advertise 10 full-duplex
- 100h - Advertise 100 half-duplex
- 100f - Advertise 100 full-duplex
- 1000f - Advertise 1000 full-duplex
- 10000f - Advertise 10000 full-duplex

- Preferred - (Optional) Specifies the master-slave preference:
  - Master - Advertise master preference
  - Slave - Advertise slave preference

Default Configuration

If capability is unspecified, defaults to list of all the capabilities of the port and preferred slave mode.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example enables auto-negotiation on te1/0/1.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# negotiation
```

16.9. flowcontrol

To configure the Flow Control on a given interface, use the `flowcontrol` Interface (Ethernet, Port Channel) Configuration mode command. To disable Flow Control, use the no form of this command.

Syntax

- flowcontrol {auto | on | off}
- no flowcontrol

Parameters

- auto - Specifies auto-negotiation of Flow Control.
- on - Enables Flow Control.
- off - Disables Flow Control.

Default Configuration

Flow control is disabled (off).

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use the `negotiation` command to enable flow control auto.

Example

The following example enables Flow Control on port te1/0/1

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# flowcontrol on
```

16.10. mdix

To enable cable crossover on a given interface, use the `mdix` Interface (Ethernet) Configuration mode command. To disable cable crossover, use the no form of this command.

Syntax

- mdix {on | auto}
- no mdix

Parameters

- on - Enables manual MDIX.
- auto - Enables automatic MDI/MDIX.

Default Configuration

The default setting is auto.

Command Mode

Interface (Ethernet) Configuration mode

Example

The following example enables automatic crossover on port te1/0/1.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# mdix auto
```

16.11. back-pressure

To enable back pressure on a specific interface, use the `back-pressure` Interface (Ethernet) Configuration mode command. To disable back pressure, use the no form of this command.

Syntax

- back-pressure
- no back-pressure

Parameters

This command has no arguments or keywords.

Default Configuration

Back pressure is disabled.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

Back-pressure cannot be enabled when EEE is enabled.

Example

The following example enables back pressure on port te1/0/1.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# back-pressure
```

16.12. port jumbo-frame

To enable jumbo frames on the device (size = 9KB), use the `port jumbo-frame` Global Configuration mode command. To disable jumbo frames, use the no form of this command.

Syntax

- port jumbo-frame
- no port jumbo-frame

Parameters

This command has no arguments or keywords.

Default Configuration

Jumbo frames are disabled on the device.

Command Mode

Global Configuration mode

User Guidelines

This command takes effect only after resetting the device.

Example

The following example enables jumbo frames on the device.

```
switchxxxxxx(config)# port jumbo-frame
```

16.13. clear counters

To clear counters on all or on a specific interface, use the `clear counters` Privileged

EXEC mode command.

Syntax

- clear counters [interface-id]

Parameters

- interface-id - (Optional) Specifies an interface ID. The interface ID can be one of the following types:
  - Ethernet port
  - Port-channel.

Default Configuration

All counters are cleared.

Command Mode

Privileged EXEC mode

Example

The following example clears the statistics counters for te1/0/1.

```
switchxxxxxx# clear counters te1/0/1
```

16.14. set interface active

To reactivate an interface that was shut down, use the `set interface active` Privileged EXEC mode command.

Syntax

- set interface active {interface-id}

Parameters

- interface-id - (Optional) Specifies an interface ID. The interface ID can be one of the following types:
  - Ethernet port
  - Port-channel.

Command Mode

Privileged EXEC mode

User Guidelines

This command is used to activate interfaces that were configured to be active, but were shut down by the system.

Example

The following example reactivates te1/0/1.

```
switchxxxxxx# set interface active te1/0/1
```

16.15. errdisable recovery cause

To enable automatic re-activation of an interface after an Err-Disable shutdown, use the `errdisable recovery cause` Global Configuration mode command. To disable automatic re-activation, use the no form of this command.

Syntax

- errdisable recovery cause {all | port-security | dot1x-src-address | acl-deny | stp-bpdu-guard | loopback-detection | storm-control | link-flap}
- no errdisable recovery cause {all | port-security | dot1x-src-address | acl-deny | stp-bpdu-guard | loopback-detection | storm-control | link-flap}

Parameters

- all - Enables the error recovery mechanism for all reasons described below.
- port-security - Enables the error recovery mechanism for the port security Err-Disable state.
- dot1x-src-address - Enables the error recovery mechanism for the 802.1x Err-Disable state.
- acl-deny - Enables the error recovery mechanism for the ACL Deny Err-Disable state.
- stp-bpdu-guard - Enables the error recovery mechanism for the STP BPDU Guard Err-Disable state.
- loopback-detection - Enables the error recovery mechanism for the Loopback Detection Err-Disable state.
- storm-control - Enables the error recovery mechanism for the Storm Control Shutdown state.
- link-flap - Enables the error recovery mechanism for link-flaps (3 or more flaps for a duration of 10 seconds).

Default Configuration

Automatic re-activation is disabled.

Command Mode

Global Configuration mode

Example

The following example enables automatic re-activation of an interface after all states.

```
switchxxxxxx(config)# errdisable recovery cause all
```

16.16. errdisable recovery interval

To set the error recovery timeout intervals use the `errdisable recovery interval` Global Configuration mode command. To return to the default configuration, use the no form of this command.

Syntax

- errdisable recovery interval seconds
- no errdisable recovery interval

Parameters

- seconds - Specifies the error recovery timeout interval in seconds. (Range: 30–86400)

Default Configuration

The default error recovery timeout interval is 300 seconds.

Command Mode

Global Configuration mode

Example

The following example sets the error recovery timeout interval to 10 minutes.

```
switchxxxxxx(config)# errdisable recovery interval 600
```

16.17. errdisable recovery reset

To reactivate one or more interfaces that were shut down by a given application, use the `errdisable recovery reset` Privileged EXEC mode command. A single interface, multiple interfaces or all interfaces can be specified.

Syntax

- errdisable recovery reset {all | port-security | dot1x-src-address | acl-deny |stp-bpdu-guard | loopback-detection | storm-control | link-flap | interface interface-id}

Parameters

- all - Reactivate all interfaces regardless of their state.
- port-security - Reactivate all interfaces in the Port Security Err-Disable state.
- dot1x-src-address - Reactivate all interfaces in the 802.1x Err-Disable state.
- acl-deny - Reactivate all interfaces in the ACL Deny Err-Disable state.
- stp-bpdu-guard - Reactivate all interfaces in the STP BPDU Guard Err-Disable state.

- loopback-detection - Reactivate all interfaces in the Loopback Detection Err-Disable state.
- storm-control - Reactivate all interfaces in the Storm Control Shutdown state.
- link-flap - Reactivate all interfaces in the link-flap Err-Disable state.
- interface interface-id - Reactivate interfaces that were configured to be active, but were shut down by the system.

Default Configuration

None.

Command Mode

Privileged EXEC mode

Examples

Example 1 - The following example reactivates interface te1/0/1:

```
switchxxxxxx# errdisable recovery reset interface te1/0/1
```

Example 2 - The following example reactivates all interfaces regardless their state:

```
switchxxxxxx# errdisable recovery reset all
```

Example 3 - The following example enables all interfaces in the port security Err-Disable state

```
switchxxxxxx# errdisable recovery reset port-security
```

16.18. show interfaces configuration

To display the configuration for all configured interfaces or for a specific interface, use the `show interfaces configuration` Privileged EXEC mode command.

Syntax

- show interfaces configuration [interface-id | detailed]

Parameters

- interface-id - (Optional) Specifies an interface ID. The interface ID can be one of the following types:
  - Ethernet port
  - Port-channel.
- detailed - (Optional) Displays information for non-present ports in addition to present ports.

Default Configuration

Display all interfaces. If detailed is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays the configuration of all configured interfaces:

```
switchxxxxxx# show interfaces configuration
  Flow Admin Back Mdix
```

```
Port Type Duplex Speed Neg control State Pressure Mode ------ -------- ------ --
--- -------- ------- ----- -------- ---te1/0/1 1G-Copper Full 1000 Disabled Off
Up Disabled Off te1/0/2 10G-Copper Full 10000 Disabled Off Up Disabled Off
  Flow Admin
PO Type Speed Neg Control State
------ ------ ----- -------- ------- -----
Po1 Disabled Off Up
switchxxxxxx# show interfaces configuration
Port Type Speed Neg Flow
 Cont
--------------------------------
te1 10G-Fiber 10000 Off On
te1 10G-Fiber 10000 Off Off
te2 10G-Fiber 10000 Off Off
```

16.19. show interfaces status

To display the status of all interfaces or of a specific interface, use the `show interfaces status` Privileged EXEC mode command.

Syntax

- show interfaces status [interface-id | detailed]

Parameters

- interface-id - (Optional) Specifies an interface ID. The interface ID can be one of the following types:
  - Ethernet port
  - Port-channel.
- detailed - (Optional) Displays information for non-present ports in addition to present ports.

Command Mode

Privileged EXEC mode

Default Configuration

Display for all interfaces. If detailed is not used, only present ports are displayed.

Example

The following example displays the status of all configured interfaces.

```
switchxxxxxx# show interfaces status
  Flow Link Back Mdix
Port Type Duplex Speed Neg ctrl State Pressure Mode
------ --------- ------ ----- -------- ---- ------ -------- ---
te1/0/1 1G-Copper Full 1000 Disabled Off Up Disabled Off
te1/0/2 1G-Copper -- -- -- -- Down -- --
  Flow Link
PO Type Duplex Speed Neg control State
----- ------- ------ ----- ------- ---- -----
Po1 1G Full 10000 Disabled Off Up *: The interface was suspended by the system.
```

16.20. show interfaces advertise

To display auto-negotiation advertisement information for all configured interfaces or for a specific interface, use the `show interfaces advertise` Privileged EXEC mode command.

Syntax

- show interfaces advertise [interface-id | detailed]

Parameters

- interface-id - (Optional) Specifies an interface ID. The interface ID can be one of the following types:
  - Ethernet port
  - Port-channel.
- detailed - (Optional) Displays information for non-present ports in addition to present ports.

Default Configuration

Display for all interfaces. If detailed is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

Examples

The following examples display auto-negotiation information.

```
switchxxxxxx# show interfaces advertise
Port Type Neg Prefered Operational Link Advertisement
---- ---------- ------ -------- -----------------------------
te1/0/1 10G-Copper Enable Master 10000f, 1000f
te1/0/2 10G-Copper Enable Slave 10000f
switchxxxxxx# show interfaces advertise te1/0/1
Port:te1/0/1
Type: 1G-Copper
Link state: Up
Auto Negotiation: enabled
Preference: Master
  10h 10f 100h 100f 1000f
  --- --- ---- ---- -----
Admin Local link Advertisement yes yes yes yes yes
Oper Local link Advertisement yes yes yes yes yes
Remote Local link Advertisement no no yes yes yes
Priority Resolution - - - - yes
switchxxxxxx# show interfaces advertise te1/0/1
Port: te1/0/1
Type: 10G-Copper
Link state: Up
Auto negotiation: disabled.
```

16.21. show interfaces description

To display the description for all configured interfaces or for a specific interface, use the `show interfaces description` Privileged EXEC mode command.

Syntax

- show interfaces description [interface-id | detailed]

Parameters

- interface-id - (Optional) Specifies an interface ID. The interface ID can be one of the following types:
  - Ethernet port
  - Port-channel.
- detailed - (Optional) Displays information for non-present ports in addition to present ports.

Default Configuration

Display description for all interfaces. If detailed is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays the description of all configured interfaces.

```
switchxxxxxx# show interfaces description
Port Descriptions
----- -------------
te1/0/1 Port that should be used for management only
te1/0/2
te1/0/3
te1/0/4
PO Description
---- -----------
Po1 Output
```

16.22. show interfaces counters

To display traffic seen by all the physical interfaces or by a specific interface, use the `show interfaces counters` Privileged EXEC mode command.

Syntax

- show interfaces counters [interface-id | detailed]

Parameters

- interface-id - (Optional) Specifies an interface ID. The interface ID can be one of the following types:
  - Ethernet port
  - port-channel.
- detailed - (Optional) Displays information for non-present ports in addition to present ports.

Default Configuration

Display counters for all interfaces. If detailed is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays traffic seen by all the physical interfaces.

```
switchxxxxxx# show interfaces counters te1/0/1
Port InUcastPkts InMcastPkts InBcastPkts InOctets ---------- ------------ ------
------ ------------ -----------te1/0/1 0 0 0 0
Port OutUcastPkts OutMcastPkts OutBcastPkts OutOctets ---------- ------------ --
---------- ------------ -----------te1/0/1 0 1 35 7051
FCS Errors: 0
Single Collision Frames: 0
Multiple Collision Frames: 0
SQE Test Errors: 0
Deferred Transmissions: 0
Late Collisions: 0
Excessive Collisions: 0
Carrier Sense Errors: 0
Oversize Packets: 0
Internal MAC Rx Errors: 0
Symbol Errors: 0
Received Pause Frames: 0
Transmitted Pause Frames: 0
```

The following table describes the fields shown in the display.

Field	Description
InOctets	Number of received octets.
InUcastPkts	Number of received Unicast packets.
InMcastPkts	Number of received Unicast packets.
InBcastPkts	Number of received broadcast packets.
OutOctets	Number of transmitted octets.
OutUcastPkts	Number of transmitted Unicast packets.
OutMcastPkts	Nmber of transmitted Unicast packets.
OutBcastPkts	Number of transmitted Broadcast packets.
FCS Errors	Number of frames received that are an integral number of octets in length but do not pass the FCS check.
Single Collision Frames	Number of frames that are involved in a single collision, and are subsequently transmitted successfully.
Multiple Collision Frames	Number of frames that are involved in more than one collision and are subsequently transmitted successfully.

SQE Test Errors	Number of times that the SQE TEST ERROR is received. The SQE TEST ERROR is set in accordance with the rules for verification of the SQE detection mechanism in the PLS Carrier Sense Function as described in IEEE Std. 802.3, 2000 Edition, section 7.2.4.6.
Deferred Transmissions	Number of frames for which the first transmission attempt is delayed because the medium is busy.
Late Collisions	Number of times that a collision is detected later than one slotTime into the transmission of a packet.
Excessive Collisions	Number of frames for which transmission fails due to excessive collisions.
Oversize Packets	Number of frames received that exceed the maximum permitted frame size.
Internal MAC Rx Errors	Number of frames for which reception fails due to an internal MAC sublayer receive error.
Field	Description
Received Pause Frames	Number of MAC Control frames received with an opcode indicating the PAUSE operation.
Transmitted Pause Frames	Number of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation.

16.23. show ports jumbo-frame

To display the whether jumbo frames are enabled on the device, use the `show ports jumbo-frame` Privileged EXEC mode command.

Syntax

- show ports jumbo-frame

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example displays whether jumbo frames are enabled on the device.

```
switchxxxxxx# show ports jumbo-frame
Jumbo frames are disabled
Jumbo frames will be enabled after reset
```

16.24. show errdisable recovery

To display the Err-Disable configuration of the device, use the `show errdisable recovery` Privileged EXEC mode command.

Syntax

- show errdisable recovery

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example displays the Err-Disable configuration.

```
switchxxxxxx# show errdisable recovery
Timer interval: 300 Seconds
Reason Automatic Recovery
---------------------- -----------------
port-security Disable
dot1x-src-address Disable
acl-deny Enable
stp-bpdu-guard Disable
stp-loopback-guard Disable
loop-detection Disable
storm control Disable
```

16.25. show errdisable interfaces

To display the Err-Disable state of all interfaces or of a specific interface, use the `show errdisable interfaces` Privileged EXEC mode command.

Syntax

- show errdisable interfaces [interface-id]

Parameters

- interface - (Optional) Port or port-channel number.

Default Configuration

Display for all interfaces.

Command Mode

Privileged EXEC mode

Example

The following example displays the Err-Disable state of te1/0/1 .

```
switchxxxxxx# show errdisable interfaces
Interface Reason
------------ -----------------
te1/0/1 stp-bpdu-guard
```

16.26. clear switchport monitor

To clear monitored statistics on all or on a specific interface or interface list, use the `clear switchport monitor` Privileged EXEC mode command.

Syntax

- clear switchport monitor [interface-id-list]

Parameters

- interface-id-list - (Optional) Specifies a list of interface ID. The interface ID can be one of the following types:
  - Ethernet port
  - Port-channel.

Default Configuration

All monitored statistics are cleared.

Command Mode

Privileged EXEC mode

Example

The following example clears the monitored statistics for te1/0/1.

```
switchxxxxxx# clear switchport monitor te1/0/1
```

16.27. show switchport monitor

To display the monitored statistics gathered by a specific interface, use the `show switchport monitor` Privileged EXEC mode command.

Syntax

- show switchport monitor interface-id {seconds | minutes | hours } [utilization | tx | rx | frames]
- show switchport monitor interface-id {days |weeks} show switchport monitor utilization [interface-id]

Parameters

- interface-id - (Optional) Specifies an interface ID. The interface ID can be one of the following types:
  - Ethernet port
  - Port-channel.
- seconds - last 20 samples, sampled every 15 seconds.
- minutes - last 60 samples, sampled every 60 seconds (every round minute according to system time).

- hours - last 24 samples, sampled every 60 minutes (every round hour according to system time).
- days - last 7 samples, sampled every 24 hours (midnight to midnight according to system time).
- weeks - last 12 samples, sampled every 7 days (midnight saturday to midnight saturday according to system time).
- utilization - shows per time frame the utilization calculated.
- rx - shows received counters statistics.
- tx - shows sent counters statistics.
- frames - show received counters statistics collected per packet size.

Default Configuration

Display monitored statistics for an interface or all interface in case of sshow switchport monitor utilization command.

Command Mode

Privileged EXEC mode

User Guidelines

The show switchport monitor utilization is used to show a utilization summary per interface of the last time frame in each time frame(i.e. last minute, last hour, last day and last week).

The show switchport monitor interface-id is used to show monitored statistics samples collected per time frame and per counter types.

Examples

Example 1 - The following example displays monitored statistics utilization seen by interface `te1/0/1`.

```
switchxxxxxx# show switchport monitor utilization te1/0/1
Interface Minutes Rx/TX Hours Rx/TX Days Rx/TX Weeks Rx/TX
 utilization utilization utilization utilization
--------- ------------ ----------- ----------- -----------
te1/0/1 95% 80% 60% 20%
```

Example 2 - The following example displays monitored Tx statistics gathered in minutes time frame seen by interface `te1/0/1`.

```
switchxxxxxx# show switchport monitor te1/0/1 minutes tx
Time Unicast frames Broadcast frames Multicast frames Good
 Dent Sent Sent Octet
   Sent
---------- -------------- ---------------- ---------------- -----
04:22:00(~) 95% 80% 60% 20%
04:23:00 80% 70% 60% 50%
```

(~) Not all samples are available.

The following table describes the fields shown in the display.

Field	Description

Time	Time stamp of the current sample in system real time clock. For seconds, minutes and hours format is: hh:mm:ss. For days and weeks format is: <day of week> dd/mm/yy.
Good Octets Received	Number of received octets.
Good Unicast frames Received	Number of received Unicast packets.
Good Multicast frames Received	Number of received Unicast packets.
Good Broadcast frames Received	Number of received broadcast packets.
Good Octets Sent	Number of transmitted octets.
Good Unicast frames Sent	Number of transmitted Unicast packets.
Good Multicast frames Sent	Nmber of transmitted Unicast packets.
Good Broadcast frames Sent	Number of transmitted Broadcast packets.
Frames of 64 bytes	Number of received packets size of 64 bytes.
Frames of 65-127 bytes	Number of received packets size of 65-127 bytes.
Frames of 128-255 bytes	Number of received packets size of 128-255 bytes.
Frames of 256-511 bytes	Number of received packets size of 256-511 bytes.
Frames of 512-1023 bytes	Number of received packets size of 512-1023 bytes.
Frames of 1024-1518 bytes	Number of received packets size of 1024-1518 bytes.
Rx Error Frames Received	Number of frames received that are an integral number of octets in length but do not pass the FCS check.
Rx Utilization	Utilization in percentage for Received frames on the interface.
Tx Utilization	Utilization in percentage for Sent frames on the interface.
Rx/Tx Utilization	An average of the Rx Utilization and the Tx Utilization in percentage on the interface.

17. Green Ethernet

17.1. green-ethernet energy-detect (global)

To enable Green-Ethernet Energy-Detect mode globally, use the `green-ethernet energy-detect` Global Configuration mode command. To disable this feature, use the no form of this command.

Syntax

- green-ethernet energy-detect
- no green-ethernet energy-detect

Parameters

This command has no arguments or keywords.

Default Configuration

Disabled.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# green-ethernet energy-detect
```

17.2. green-ethernet energy-detect (interface)

Use the `green-ethernet energy-detect` Interface configuration mode command to enable Green Ethernet-Energy-Detect mode on a port. Use the no form of this command, to disable it on a port.

Syntax

- green-ethernet energy-detect
- no green-ethernet energy-detect

Parameters

This command has no arguments or keywords.

Default Configuration

- Gigabit and Fast Ethernet ports: disabled.
- XG and MultiGig Ethernet ports: disabled.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

Energy-Detect only works on copper ports. When a port is enabled for auto selection, copper/fiber Energy-Detect cannot work.

It takes the PHY ~5 seconds to fall into sleep mode when the link is lost after normal operation.

Example

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# green-ethernet energy-detect
```

17.3. green-ethernet short-reach (global)

Use the `green-ethernet short-reach` Global Configuration mode command to enable Green-Ethernet Short-Reach mode globally. Use the no form of this command to disabled it.

Note:
Short reach threshold for power reduction works with cable length less than 50m.

Syntax

- green-ethernet short-reach
- no green-ethernet short-reach

Parameters

This command has no arguments or keywords.

Default Configuration

Disabled.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# green-ethernet short-reach
```

17.4. green-ethernet short-reach (interface)

Use the `green-ethernet short-reach` Interface Configuration mode command to enable green-ethernet short-reach mode on a port. Use the no form of this command to disable it on a port.

Syntax

- green-ethernet short-reach
- no green-ethernet short-reach

Parameters

This command has no arguments or keywords.

Default Configuration

- Gigabit and Fast Ethernet ports: disabled.
- XG and MultiGig Ethernet ports: enabled.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

The VCT length check can be performed only on a copper port operating at a speed of 1000 Mbps. If the media is not copper or the link speed is not 1000, Mbps Short-Reach mode is not applied.

When the interface is set to enhanced mode, after the VCT length check has completed and set the power to low, an active monitoring for errors is done continuously. In the case of errors crossing a certain threshold, the PHY will be reverted to long reach.

Note that EEE cannot be enabled if the Short-Reach mode is enabled.

Example

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# green-ethernet short-reach
```

17.5. green-ethernet power-meter reset

Use the `green-ethernet power meter reset` Privileged EXEC mode command to reset the power save meter.

Syntax

- green-ethernet power-meter reset

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# green-ethernet power-meter reset
```

17.6. show green-ethernet

To display green-ethernet configuration and information, use the `show green-ethernet` Privileged EXEC mode command.

Syntax

- show green-ethernet [interface-id | detailed]

Parameters

- interface-id - (Optional) Specifies an Ethernet port
- detailed - (Optional) Displays information for non-present ports in addition to present ports.

Default Configuration

Display for all ports. If detailed is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

User Guidelines

The power savings displayed is relevant to the power saved by:

- Energy detect
- Short reach

The EEE power saving is dynamic by nature since it is based on port utilization and is therefore not taken into consideration.

The following describes the reasons for non-operation displayed by this command.

If there are a several reasons, then only the highest priority reason is displayed.

Energy-Detect Non-Operational Reasons		
Priority	Reason	Description
1	NP	Port is not present
2	LT	Link Type is not supported (fiber, auto media select)
3	LU	Port Link is up – NA

Example

Short-Reach Non-Operational Reasons		
Priority	Reason	Description
1	NP	Port is not present
2	LT	Link Type is not supported (fiber)
3	LS	Link Speed Is not Supported (10mbps,100mbps)
4	LL	Link Length received from VCT test exceeds threshold
6	LD	Port Link is Down – NA

```
switchxxxxxx# show green-ethernet
Energy-Detect mode: Enabled
Short-Reach mode: Disabled
Power Savings: 24% (1.08W out of maximum 4.33W)
Cumulative Energy Saved: 33 [Watt*Hour]
Short-Reach cable length threshold: 50m
Port       Energy-Detect       Short-Reach            VCT Cable
         Admin Oper Reason   Admin Force Oper Reason   Length
----     ----- ---- -------  ----- ----- ---- -------  -----
te1/0/1   on    on           off   off   off
te1/0/2   on    off  LU      on    off   on            < 50
te1/0/3   on    off  LU      off   off   off
```

18. GARP VLAN Registration Protocol (GVRP) Commands

18.1. clear gvrp statistics

To clear GVRP statistical information for all interfaces or for a specific interface, use the `clear gvrp statistics` Privileged EXEC mode command.

Syntax

- clear gvrp statistics [interface-id]

Parameters

- Interface-id - (Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

All GVRP statistics are cleared.

Command Mode

Privileged EXEC mode

Example

The following example clears all GVRP statistical information on `te1/0/4`.

```
switchxxxxxx# clear gvrp statistics te1/0/4
```

18.2. gvrp enable (Global)

To enable the Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) globally, use the `gvrp enable` Global Configuration mode command. To disable GVRP on the device, use the no form of this command.

Syntax

- gvrp enable
- no gvrp enable

Parameters

This command has no arguments or keywords.

Default Configuration

GVRP is globally disabled.

Command Mode

Global Configuration mode

Example

The following example enables GVRP globally on the device.

```
switchxxxxxx(config)# gvrp enable
```

18.3. gvrp enable (Interface)

To enable GVRP on an interface, use the `gvrp enable` Interface (Ethernet, Port Channel) Configuration mode command. To disable GVRP on an interface, use the no form of this command.

Syntax

- gvrp enable
- no gvrp enable

Parameters

This command has no arguments or keywords.

Default Configuration

GVRP is disabled on all interfaces.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

An access port does not dynamically join a VLAN because it is always a member of a single VLAN only. Membership in an untagged VLAN is propagated in the same way as in a tagged VLAN. That is, the PVID must be manually defined as the untagged VLAN ID.

Example

The following example enables GVRP on `te1/0/`4.

```
switchxxxxxx(config)# interface te1/0/4
switchxxxxxx(config-if)# gvrp enable
```

18.4. garp timer

To adjust the values of the join, leave and leaveall timers of GARP applications, such as GVRP, use the `garp timer` Interface Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- garp timer {join | leave | leaveall} timer-value
- no garp timer

Parameters

The following specify the type of timer. The possible values are:

- join - Specifies the GARP join timer. The timer value for this type of timer specifies the time interval between the two join messages sent by the GARP application.
- leave - Specifies the GARP leave timer. The timer value for this type of timer specifies the time interval for a GARP application to wait for a join message after receiving a leave message for a GARP attribute, before it de-registers the GARP attribute.
- leaveall - Specifies the GARP leaveall timer. The timer value for this type of timer specifies the time interval between leaveall messages for a GARP entity, which prompt other GARP entities to re-reregister all attribute information on this entity.
- timer-value - Specifies the timer value in milliseconds in multiples of 10. (Range: 10–2147483640)

Default Configuration

The following are the default timer values:

- Join timer - 200 milliseconds
- Leave timer - 600 milliseconds
- Leaveall timer - 10000 milliseconds

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The timer-value must be a multiple of 10.

The following relationship must be maintained between the timers:

- The leave timer value must be greater than or equal to three times the join timer.
- The leave-all timer value must be greater than the leave timer.

Set the same GARP timer values on all Layer 2-connected devices to ensure proper operation of the GARP application.

Example

The following example sets the leave timer for `te1/0/`4 to 900 milliseconds.

```
switchxxxxxx(config-if)# interface te1/0/4
switchxxxxxx(config-if)# garp timer leave 900
```

18.5. gvrp registration-forbid

To deregister all dynamic VLANs on a port and prevent VLAN creation or registration on the port, use the `gvrp registration-forbid` Interface Configuration mode command. To allow dynamic registration of VLANs on a port, use the no form of this command.

Syntax

- gvrp registration-forbid
- no gvrp registration-forbid

Parameters

This command has no arguments or keywords.

Default Configuration

Dynamic registration of VLANs on the port is allowed.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example forbids dynamic registration of VLANs on `te1/0/`2.

```
switchxxxxxx(config-if)# interface te1/0/2
switchxxxxxx(config-if)# gvrp registration-forbid
```

18.6. gvrp vlan-creation-forbid

To disable dynamic VLAN creation or modification, use the `gvrp vlan-creation-forbid` Interface Configuration mode command. To enable dynamic VLAN creation or modification, use the no form of this command.

Syntax

- gvrp vlan-creation-forbid
- no gvrp vlan-creation-forbid

Parameters

This command has no arguments or keywords.

Default Configuration

Enabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example disables dynamic VLAN creation on `te1/0/3`.

```
switchxxxxxx(config-if)# interface te1/0/3
switchxxxxxx(config-if)# gvrp vlan-creation-forbid
```

18.7. show gvrp configuration

To display GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation are enabled, and which ports are running GVRP, use the `show gvrp configuration` EXEC mode command.

Syntax

- show gvrp configuration [interface-id | detailed]

Parameters

- interface-id - (Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- detailed - (Optional) Displays information for non-present ports in addition to present ports.

Default Configuration

All GVRP statistics are displayed for all interfaces. If detailed is not used, only present ports are displayed.

Command Mode

User EXEC mode

Example

The following example displays GVRP configuration.

```
switchxxxxxx# show gvrp configuration
GVRP Feature is currently Enabled on the device.
Maximum VLANs: 4094
Port(s) GVRP-Status Regist- Dynamic Timers(ms)
```

```
 ration VLAN Creation Join Leave Leave All
---- ----------- -------- ------------- ---- ----- ---------
te1/0/1 Enabled Forbidden Disabled 600 200 10000 te1/0/2 Enabled Normal Enabled
1200 400 20000
```

18.8. show gvrp error-statistics

Use the `show gvrp error-statistics` EXEC mode command to display GVRP error statistics for all interfaces or for a specific interface.

Syntax

- show gvrp error-statistics [interface-id]

Parameters

- interface-id - (Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

All GVRP error statistics are displayed.

Command Mode

User EXEC mode

Example

The following example displays GVRP error statistics.

```
switchxxxxxx# show gvrp error-statistics
GVRP Error Statistics:
----------------------
Legend:
 INVPROT : Invalid Protocol Id
 INVATYP : Invalid Attribute Type INVALEN : Invalid Attribute Length
 INVAVAL : Invalid Attribute Value INVEVENT: Invalid Event
Port INVPROT INVATYP INVAVAL INVALEN INVEVENT
-------- ------- ------- ------- ------- -------
te1/0/1 0 0 0 0 0
te1/0/2 0 0 0 0 0
te1/0/3 0 0 0 0 0
te1/0/4 0 0 0 0 0
```

18.9. show gvrp statistics

To display GVRP statistics for all interfaces or for a specific interface, use the `show gvrp statistics` EXEC mode command.

Syntax

- show gvrp statistics [interface-id]

Parameters

- interface-id - (Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

All GVRP statistics are displayed.

Command Mode

User EXEC mode

Example

```
The following example displays GVRP statistical information.
switchxxxxxx# show gvrp statistics
GVRP statistics:
---------------
Legend:
rJE: Join Empty Received rEmp: Empty Received rLE: Leave Empty Received
sJE: Join Empty Sent sEmp: Empty Sent sLE: Leave Empty Sent
Port rJE rJIn rEmp rLIn
----- --- ---- ---- ---
te1/0/1 0 0 0 0
te1/0/2 0 0 0 0
te1/0/3 0 0 0 0
te1/0/4 0 0 0 0
rJIn: Join In Received rLIn: Leave In Received rLA : Leave All Received sJIn:
Join In Sent sLIn: Leave In Sent sLA : Leave All Sent
rLE rLA sJE sJIn sEmp sLIn sLE sLA
--- --- --- ---- ---- ---- --- ---
0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
```

19. IGMP Commands

19.1. clear ip igmp counters

To clear the Internet Group Management Protocol (IGMP) interface counters, use the `clear ip igmp counters` command in Privileged EXEC mode.

Syntax

- clear ip igmp counters [interface-id]

Parameters

- interface-id - (Optional) Interface Identifier

Command Mode

Privileged EXEC mode

User Guidelines

Use the `clear ip igmp counters` command to clear the IGMP counters, which keep track of the number of joins and leaves received. If you omit the optional interface-id argument, the clear ip igmp counters command clears the counters on all interfaces.

Example

The following example clears the counters for VLAN 100:

```
switchxxxxxx# clear ip igmp counters vlan 100
```

19.2. ip igmp last-member-query-count

To configure the Internet Group Management Protocol (IGMP) last member query counter, use the `ip igmp last-member-query-count` command in Interface Configuration mode. To restore the default value, use the no form of this command.

Syntax

- ip igmp last-member-query-count count
- no ip igmp last-member-query-count

Parameters

- count - The number of times that group- or group-source-specific queries are sent upon receipt of a message indicating a leave. (Range: 1–7)

Default Configuration

A value of IGMP Robustness variable.

Command Mode

Interface Configuration mode

User Guidelines

Use the `ip igmp robustness` command to change the IGMP last member query counter.

Example

The following example changes a value of the IGMP last member query counter to 3:

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip igmp last-member-query-count 3
switchxxxxxx(config-if)# exit
```

19.3. ip igmp last-member-query-interval

To configure the Internet Group Management Protocol (IGMP) last member query interval, use the `ip igmp last-member-query-interval` command in Interface Configuration mode. To restore the default IGMP query interval, use the no form of this command.

Syntax

- ip igmp last-member-query-interval milliseconds
- no ip igmp last-member-query-interval

Parameters

- milliseconds - Interval, in milliseconds, at which IGMP group-specific host query messages are sent on the interface. (Range: 100–25500).

Default Configuration

The default IGMP last member query interval is 1000 milliseconds.

Command Mode

Interface Configuration mode

User Guidelines

Use the `ip igmp last-member-query-interval` command to configure the IGMP last member query interval on an interface.

Example

The following example shows how to increase the the IGMP last member query interval to 1500 milliseconds:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ip igmp last-member-query-interval 1500
switchxxxxxx(config-if)# exit
```

19.4. ip igmp query-interval

To configure the frequency at which the IGMP querier sends Internet Group Management Protocol (IGMP) host-query messages from an interface, use the `ip igmp query-interval` command in Interface Configuration mode. To restore the default IGMP query interval, use the no form of this command.

Syntax

- ip igmp query-interval seconds
- no ip igmp query-interval

Parameters

- seconds - Frequency, in seconds, at which the switch sends IGMP query messages from the interface. The range is from 30 to 18000.

Default Configuration

The default IGMP query interval is 125 seconds.

Command Mode

Interface Configuration mode

User Guidelines

Use the `ip igmp query-interval` command to configure the frequency at which the IGMP querier sends IGMP host-query messages from an interface. The IGMP querier sends query-host messages to discover which multicast groups have members on the attached networks of the router.

The query interval must be bigger than the maximum query response time.

Example

The following example shows how to increase the frequency at which the IGMP querier sends IGMP host-query messages to 180 seconds:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ip igmp query-interval 180
switchxxxxxx(config-if)# exit
```

19.5. ip igmp query-max-response-time

To configure the maximum response time advertised in Internet Group Management Protocol (IGMP) queries, use the `ip igmp query-max-response-time` command in Interface Configuration mode. To restore the default value, use the no form of this command.

Syntax

- ip igmp query-max-response-time seconds
- no ip igmp query-max-response-time

Parameters

- seconds - Maximum response time, in seconds, advertised in IGMP queries. (Range: 5–20)

Default Configuration

10 seconds.

Command Mode

Interface Configuration mode

User Guidelines

This command controls the period during which the responder can respond to an IGMP query message before the router deletes the group.

This command controls how much time the hosts have to answer an IGMP query message before the router deletes their group. Configuring a value of fewer than 10 seconds enables the router to prune groups faster.

The maximum query response time must be less than the query interval.

Note. If the hosts do not respond fast enough, they might be pruned inadvertently. Therefore, the hosts must know to respond faster than 10 seconds (or the value you configure).

Example

The following example configures a maximum response time of 8 seconds:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ip igmp query-max-response-time 8
switchxxxxxx(config-if)# exit
```

19.6. ip igmp robustness

To configure the Internet Group Management Protocol (IGMP) robustness variable, use the `ip igmp robustness` command in Interface Configuration mode. To restore the default value, use the no form of this command.

Syntax

- ip igmp robustness count
- no ip igmp robustness

Parameters

- count - The number of expected packet loss on a link. Parameter range. (Range: 1–7).

Default Configuration

The default value is 2.

Command Mode

Interface Configuration mode

User Guidelines

Use the `ip igmp robustness` command to change the IGMP robustness variable.

Example

The following example changes a value of the IGMP robustness variable to 3:

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip igmp robustness 3
switchxxxxxx(config-if)# exit
```

19.7. ip igmp version

To configure which version of Internet Group Management Protocol (IGMP) the router uses, use the `ip igmp version` command in Interface Configuration mode. To restore the default value, use the no form of this command.

Syntax

- ip igmp version {1 | 2 | 3}
- no ip igmp version

Parameters

- 1 - IGMP Version 1.
- 2 - IGMP Version 2.
- 3 - IGMP Version 3.

Default Configuration

2

Command Mode

Interface Configuration mode

User Guidelines

Use the commnad to change the default version of IGMP>

Example

The following example configures the router to use IGMP Version 2:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ip igmp version 2
switchxxxxxx(config-if)# exit
```

19.8. show ip igmp counters

To display the Internet Group Management Protocol (IGMP) traffic counters, use the `show ip igmp counters` command in User EXEC mode.

Syntax

- show ip igmp counters [interface-id]

Parameters

- interface-id - (Optional) Interface Identifier.

Command Mode

User EXEC mode

User Guidelines

Use the `show ip igmp counters` command to check if the expected number of IGMP protocol messages have been received and sent.

If you omit the optional interface-id argument, the show ip igmp counters command displays counters of all interfaces.

Example

The following example displays the IGMP protocol messages received and sent:

```
switchxxxxxx# show ip igmp counters vlan 100
VLAN 100
 Elapsed time since counters cleared:00:00:21
 Failed received Joins: 0
 Total IGMPv1 received messages: 0
 Total IGMPv2 received messages: 10
 Total IGMPv3 received messages: 0
 Total invalid received messages: 0
 General Sent Queries: 0
 Specific Sent Queries: 0
```

19.9. show ip igmp groups

To display the multicast groups that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP), use the `show ip igmp groups` command in User EXEC mode.

Syntax

- show ip igmp groups [group-name | group-address | interface-id] [detail]

Parameters

- group-name | group-address - (Optional) IP address or name of the multicast group.
- interface-id - (Optional) Interface identifier.
- detail - (Optional) Displays detailed information about individual sources.

Command Mode

User EXEC mode

User Guidelines

Use the show ip igmp groups [detail] command to display all directly connected groups.

Use the show ip igmp groups [group-name | group-address] [detail] command to display one given directly connected group.

Use the show ip igmp groups interface-id [detail] command to display all groups directly connected to the given interface.

Examples

Example 1. The following is sample output from the show ip igmp groups command. It shows all of the groups joined by VLAN 100:

```
switchxxxxxx# show ip igmp groups vlan 100
IGMP Connected Group Membership
Expires: never - switch itself has joined the group
Group Address Interface Expires
224.1.1.1 VLAN 100 00:01:30
224.10.12.79 VLAN 100 never
225.1.1.1 VLAN 100 00:00:27
```

Example 2. The following is sample output from the show ip igmp groups command using the detail keyword:

```
switchxxxxxx# show ip igmp groups detail
Expires: zero value - INCLUDE state; non-zero value - EXCLUDE state
Interface: VLAN 100
 Group: 225.1.1.1
 Router mode: INCLUDE
 Last reporter: 10.0.119.133 Group Timer Expires: 00:20:11
 Group source list:
 Source Address  Expires
 20.1.1.1  00:04:08
 120.1.1.1  00:02:01
 Group: 226.1.1.2
 Router mode: EXCLUDE
 Last reporter: 100.1.12.130
 Group Timer Expiry: 00:22:12
 Exclude Mode Expiry (Filter) Timer: 00:10:11 Group source list:
 Source Address  Expires
 2.2.2.1  00:04:08
 192.168.1.1  00:04:08
 12.1.1.10  00:00:00
```

```
 40.3.4.2  00:00:00
```

19.10. show ip igmp groups summary

To display the number of (*, G) and (S, G) membership reports present in the Internet Group Management Protocol (IGMP) cache, use the `show ip igmp groups summary` command in User EXEC mode.

Syntax

- show ip igmp groups summary

Parameters

This command has no arguments or keywords.

Command Mode

User EXEC mode

User Guidelines

The show ip igmp groups summary command displays the number of directly connected multicast groups.

Example

The following is sample output from the show ip igmp groups summary command:

```
switchxxxxxx# show ip igmp groups summary
IGMP Route Summary
 No. of (*,G) routes = 5
 No. of (S,G) routes = 0
Field Descriptions:
No. of (*,G) routes = 5 - Displays the number of groups present in the IGMP
cache.
No. of (S,G) routes = 0 - Displays the number of include and exclude mode
sources present in the IGMP cache.
```

19.11. show ip igmp interface

To display multicast-related information about an interface, use the `show ip igmp interface` command in User EXEC mode.

Syntax

- show ip igmp interface [interface-id]

Parameters

- interface-id - (Optional) Interface identifier.

Command Mode

User EXEC mode

User Guidelines

If you omit the optional interface-id argument, the show ip igmp interface command displays information about all interfaces.

Example

The following is sample output from the show ip igmp interface command for Ethernet interface 2/1/1:

```
switchxxxxxx# show ip igmp interface vlan 100
VLAN 100 is up
 Administrative IGMP Querier IP address is 1.1.1.1
 Operational IGMP Querier IP address is 1.1.1.1
 Current IGMP version is 3
 Administrative IGMP robustness variable is 2 seconds Operational IGMP
robustness variable is 2 seconds
 Administrative IGMP query interval is 125 seconds
 Operational IGMP query interval is 125 seconds
 Administrative IGMP max query response time is 10 seconds
 Operational IGMP max query response time is 10 seconds
 Administrative Last member query response interval is 1000 milliseconds
Operational Last member query response interval is 1000 milliseconds
```

20. IGMP Proxy Commands

20.1. ip igmp-proxy

To add downstream interfaces to an IGMP proxy tree, use the `ip igmp-proxy` command in Interface Configuration mode. To remove downstream from interfaces to an IGMP proxy tree, use the no form of this command.

Syntax

- ip igmp-proxy upstream-interface-id
- no ip igmp-proxy

Parameters

- upstream-interface-id - Upstream Interface identifier.

Default Configuration

The protocol is disabled on the interface.

Command Mode

Interface Configuration mode

User Guidelines

Use the `ip igmp-proxy` command to add downstream interfaces to an IGMP proxy tree. If the proxy tree does not exist it is created.

Use the no format of the command to remove the downstream interface. When the last downstream interface is removed from the proxy tree it is deleted too.

Examples

Example 1. The following example adds a downstream interface to an IGMP Proxy process with vlan 200 as its Upstream interface:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ip igmp-proxy vlan 200
switchxxxxxx(config-if)# exit
```

Example 2. The following example adds a range of downstream interfaces to an IGMP Proxy process with vlan 200 as its Upstream interface:

```
switchxxxxxx(config)# interface range vlan 100-105
switchxxxxxx(config-if)# ip igmp-proxy vlan 200
switchxxxxxx(config-if)# exit
```

20.2. ip igmp-proxy downstream protected

To disable forwarding of IP Multicast traffic from downstream interfaces, use the `ip igmp-proxy downstream protected` command in Global Configuration mode. To allow forwarding from downstream interfaces, use the no form of this command.

Syntax

- ip igmp-proxy downstream protected
- no ip igmp-proxy downstream protected

Parameters

This command has no arguments or keywords.

Default Configuration

Forwarding from downstream interfaces is allowed.

Command Mode

Global Configuration mode

User Guidelines

Use the `ip igmp-proxy downstream protected` command to block forwarding from downstream interfaces.

Example

The following example prohibits forwarding from downstream interfaces:

```
switchxxxxxx(config)# ip igmp-proxy downstream protected
```

20.3. ip igmp-proxy downstream protected interface

To disable or enable forwarding of IP Multicast traffic from a given downstream interface, use the `ip igmp-proxy downstream protected interface` command in Interface Configuration mode. To return to default, use the no form of this command.

Syntax

- ip igmp-proxy downstream protected interface {enabled | disabled}
- no ip igmp-proxy downstream protected interface

Parameters

- enabled - Downstream interface protection on the interface is enabled. IPv4 Multicast traffic arriving on the interface will not be forwarded.
- disabled - Downstream interface protection on the interface is disabled.

IPv4 Multicast traffic arriving on the interface will be forwarded.

Default Configuration

Global downstream protection configuration (see the ip igmp-proxy downstream protected command)

Command Mode

Interface Configuration mode

User Guidelines

Use the `ip igmp-proxy downstream protected interface disabled` command to block forwarding from the given downstream interface.

Use `the ip igmp-proxy downstream protected interface enabled` command to allow forwarding from the given downstream interface.

The command can be configured only for a downstream interface. When a downstream interface is removed from the IGMP Proxy tree the configuration is removed too.

Example

The following example prohibits forwarding from downstream interface vlan 100:

```
switchxxxxxx(config)# interface vlan100
switchxxxxxx(config-if)# ip igmp-proxy downstream protected interface enabled
switchxxxxxx(config-if)# exit
```

20.4. ip igmp-proxy ssm

To define the Source Specific Multicast (SSM) range of IP Multicast addresses, use the `ip igmp-proxy ssm` command in Global Configuration mode. To disable the SSM range, use the no form of this command.

Syntax

- ip igmp-proxy ssm {default | range access-list}
- no ip igmp-proxy ssm

Parameters

- default - Defines the SSM range access list to 232.0.0.0/8 (see rfc4607).
- range access-list - Specifies the standard IP access list name defining the SSM range.

Default Configuration

The command is disabled.

Command Mode

Global Configuration mode

User Guidelines

A new ip igmp-proxy ssm command overrides the previous ip igmp-proxy ssm command.

Use the no ip igmp-proxy ssm command to remove all defined ranges.

Example

The following example shows how to configure SSM service for the default IP address range and the IP address ranges defined by access list list1:

```
switchxxxxxx(config)# ip access-list list1 permit 224.2.151.0/24
switchxxxxxx(config)# ip access-list list1 deny 224.2.152.141
switchxxxxxx(config)# ip access-list list1 permit 224.2.152.0/24
switchxxxxxx(config)# ip igmp-proxy ssm range list1
```

20.5. show ip igmp-proxy interface

To display information about interfaces configured for IGMP Proxy, use the `show ip igmp-proxy interface` command in User EXEC mode or Privileged EXEC mode.

Syntax

- show ip igmp-proxy interface [interface-id]

Parameters

- interface-id - (Optional) Display IGMP Proxy information about the interface.

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

The show ip igmp-proxy interface command is used to display all interfaces where the IGMP Proxy is enabled or to display the IGMP Proxy configuration for a given interface.

Examples

Example 1. The following example displays IGMP Proxy status on all interfaces where the IGMP Proxy is enabled:

```
switchxxxxxx# show ip igmp-proxy interface
* - the switch is the Querier on the interface
IP Forwarding is enabled
IP Multicast Routing is enabled
IGMP Proxy is enabled
Global Downdtream interfaces protection is disabled
SSM Access List Name:list1
Interface Type Interface Protection vlan 100 upstream
*vlan 102 downstream enabled *vlan 110 downstream default vlan 113 downstream
disabled
```

Example 2. The following is sample output from the show ip igmp-proxy interface command for given upstream interface:

```
switchxxxxxx# show ip igmp-proxy interface vlan 100
* - the switch is the Querier on the interface
IP Forwarding is enabled
IP Multicast Routing is enabled
IGMP Proxy is enabled
Global Downdtream interfaces protection is disabled SSM Access List Name:
IP Multicast Tarffic Discarding from Downdtream interfaces is disabled vlan 100
is a Upstream interface Downstream interfaces:
 *vlan 102, *vlan 110, vlan 113
```

Example 3. The following is sample output from the show ip igmp-proxy interface command for given downstream interface:

```
switchxxxxxx# show ip igmp-proxy interface vlan 102
IP Forwarding is enabled
IP Multicast Routing is enabled
IGMP Proxy is enabled
Global Downdtream interfaces protection is disabled vlan 102 is a Downstream
interface
The switch is the Querier on vlan 102
Downsteam Interface protection is enabled
SSM Access List Name: default
Upstream interface: vlan 100
```

Example 4. The following is sample output from the show ip igmp-proxy interface command for an interface on which IGMP Proxy is disabled:

```
switchxxxxxx# show ip igmp-proxy interface vlan 1
IP Forwarding is enabled
IP Multicast Routing is enabled
IGMP Proxy is disabled
```

21. IGMP Snooping Commands

21.1. ip igmp snooping (Global)

To enable Internet Group Management Protocol (IGMP) snooping, use the `ip igmp snooping` command in Global Configuration mode. To return to the default, use the no form of this command.

Syntax

- ip igmp snooping
- no ip igmp snooping

Default Configuration

Disabled.

Command Mode

Global Configuration mode

Example

The following example enables IGMP snooping.

```
switchxxxxxx(config)# ip igmp snooping
```

21.2. ip igmp snooping vlan

To enable IGMP snooping on a specific VLAN, use the `ip igmp snooping vlan` command in Global Configuration mode. To return to the default, use the no form of this command.

Syntax

- ip igmp snooping vlan vlan-id
- no ip igmp snooping vlan vlan-id

Parameters

- vlan-id - Specifies the VLAN.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

IGMP snooping can be enabled only on static VLANs.

IGMPv1, IGMPv2, and IGMPv3 Snooping are supported.

To activate IGMP snooping, bridge multicast filtering must be enabled by the `bridge multicast filtering` command.

The user guidelines of the `bridge multicast mode` command describes the configuration that is written into the FDB as a function of the FDB mode and the IGMP version that is used in the network.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 2
```

21.3. ip igmp snooping vlan mrouter

To enable automatic learning of Multicast router ports on a VLAN, use the `ip igmp snooping vlan mrouter` command in Global Configuration mode. To remove the configuration, use the no form of this command.

Syntax

- ip igmp snooping vlan vlan-id mrouter learn pim-dvmrp
- no ip igmp snooping vlan vlan-id mrouter learn pim-dvmrp

Parameters

- vlan-id - Specifies the VLAN.

Default Configuration

Learning pim-dvmrp is enabled.

Command Mode

Global Configuration mode

User Guidelines

Multicast router ports are learned according to:

- Queries received on the port
- PIM/PIMv2 received on the port
- DVMRP received on the port
- MRDISC received on the port
- MOSPF received on the port

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
```

21.4. ip igmp snooping vlan mrouter interface

To define a port that is connected to a Multicast router port, use the `ip igmp snooping mrouter interface` command in Global Configuration mode. To return to the default, use the no form of this command.

Syntax

- ip igmp snooping vlan vlan-id mrouter interface interface-list
- no ip igmp snooping vlan vlan-id mrouter interface interface-list

Parameters

- vlan-id - Specifies the VLAN.
- interface-list - Specifies the list of interfaces. The interfaces can be one of the following types: Ethernet port or Port-channel.

Default Configuration

No ports defined

Command Mode

Global Configuration mode

User Guidelines

A port that is defined as a Multicast router port receives all IGMP packets (reports and queries) as well as all Multicast data.

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 mrouter interface te1/0/1
```

21.5. ip igmp snooping vlan forbidden mrouter

To forbid a port from being defined as a Multicast router port by static configuration or by automatic learning, use the `ip igmp snooping vlan forbidden mrouter` command in Global Configuration mode. To return to the default, use the no form of this command.

Syntax

- ip igmp snooping vlan vlan-id forbidden mrouter interface interface-list
- no ip igmp snooping vlan vlan-id forbidden mrouter interface interface-list

Parameters

- vlan-id - Specifies the VLAN.
- interface-list - Specifies a list of interfaces. The interfaces can be of one of the following types:
  - Ethernet port
  - Port-channel.

Default Configuration

No ports defined.

Command Mode

Global Configuration mode

User Guidelines

A port that is a forbidden mrouter port cannot be a Multicast router port (i.e. cannot be learned dynamically or assigned statically).

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 forbidden mrouter interface
te1/0/1
```

21.6. ip igmp snooping vlan static

To register an IP-layer Multicast address to the bridge table, and to add static ports to the group defined by this address, use the `ip igmp snooping vlan static` command in Global Configuration mode. To return to the default, use the no form of this command.

Syntax

- ip igmp snooping vlan vlan-id static ip-address [interface interface-list]

- no ip igmp snooping vlan vlan-id static ip-address [interface interface-list]

Parameter

- vlan-id - Specifies the VLAN.
- ip-address - Specifies the IP Multicast address.
- interface interface-list - (Optional) Specifies a list of interfaces. The interfaces can be of one of the following types: Ethernet port or Port-channel.

Default Configuration

No Multicast addresses are defined.

Command Mode

Global Configuration mode

User Guidelines

Static Multicast addresses can only be defined on static VLANs.

You can execute the command before the VLAN is created.

You can register an entry without specifying an interface.

Using the no command without a port-list removes the entry.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 static 239.2.2.2 interface te1/0/1
```

21.7. ip igmp snooping vlan multicast-tv

To define the Multicast IP addresses that are associated with a Multicast TV VLAN, use the `ip igmp snooping vlan multicast-tv` command in Global Configuration mode. To return to the default, use the no form of this command.

Syntax

- ip igmp snooping vlan vlan-id multicast-tv ip-multicast-address [count number]
- no ip igmp snooping vlan vlan-id multicast-tv ip-multicast-address [count number]

Parameters

- vlan-id - Specifies the VLAN
- ip-multicast-address - Multicast IP address
- count number - (Optional) Configures multiple contiguous Multicast IP addresses. If not specified, the default is 1. (Range: 1–256)

Default Configuration

No Multicast IP address is associated.

Command Mode

Global Configuration mode

User Guidelines

Use this command to define the Multicast transmissions on a Multicast-TV VLAN. The configuration is only relevant for an Access port that is a member in the configured VLAN as a Multicast-TV VLAN.

If an IGMP message is received on such an Access port, it is associated with the Multicast-TV VLAN only if it is for one of the Multicast IP addresses that are associated with the Multicast-TV VLAN.

Up to 256 VLANs can be configured.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 multicast-tv 239.2.2.2 count 3
```

21.8. ip igmp snooping map cpe vlan

To map CPE VLANs to Multicast-TV VLANs, use the `ip igmp snooping map cpe vlan` command in Global Configuration mode. To return to the default, use the no form of this command.

Syntax

- ip igmp snooping map cpe vlan cpe-vlan-id multicast-tv vlan vlan-id
- no ip igmp snooping map cpe vlan vlan-id

Parameters

- cpe-vlan-id - Specifies the CPE VLAN ID.
- vlan-id - Specifies the Multicast-TV VLAN ID.

Default Configuration

No mapping exists.

Command Mode

Global Configuration mode

User Guidelines

Use this command to associate the CPE VLAN with a Multicast-TV VLAN.

If an IGMP message is received on a customer port tagged with a CPE VLAN, and there is mapping from that CPE VLAN to a Multicast-TV VLAN, the IGMP message is associated with the Multicast-TV VLAN.

Example

The following example maps CPE VLAN 2 to Multicast-TV VLAN 31.

```
switchxxxxxx(config)# ip igmp snooping map cpe vlan 2 multicast-tv vlan 31
```

21.9. ip igmp snooping querier

To enable globally the IGMP Snooping querier, use the `ip igmp snooping querier` command in Global Configuration mode. To disable the IGMP Snooping querier globally, use the no form of this command.

Syntax

- ip igmp snooping querier
- no ip igmp snooping querier

Parameters

N/A

Default Configuration

Enabled

Command Mode

Global Configuration mode

User Guidelines

To run the IGMP Snooping querier on a VLAN, you have enable it globally and on the VLAN.

Example

The following example disables the IGMP Snooping querier globally:

```
switchxxxxxx(config)# no ip igmp snooping querier
```

21.10. ip igmp snooping vlan querier

To enable the IGMP Snooping querier on a specific VLAN, use the `ip igmp snooping vlan querier` command in Global Configuration mode. To disable the IGMP Snooping querier on the VLAN interface, use the no form of this command.

Syntax

- ip igmp snooping vlan vlan-id querier
- no ip igmp snooping vlan vlan-id querier

Parameters

- vlan-id - Specifies the VLAN.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

The IGMP Snooping querier can be enabled on a VLAN only if IGMP Snooping is enabled for that VLAN.

Example

The following example enables the IGMP Snooping querier on VLAN 1:

```
switchxxxxxx(config)# ip igmp snooping vlan 1 querier
```

21.11. ip igmp snooping vlan querier address

To define the source IP address that the IGMP snooping querier uses, use the `ip igmp snooping vlan querier address` command in Global Configuration mode. To return to the default, use the no form of this command.

Syntax

- ip igmp snooping vlan vlan-id querier address ip-address
- no ip igmp snooping vlan vlan-id querier address

Parameters

- vlan-id - Specifies the VLAN.
- ip-address - Source IP address.

Default Configuration

If an IP address is configured for the VLAN, it is used as the source address of the IGMP snooping querier. If there are multiple IP addresses, the minimum IP address defined on the VLAN is used.

Command Mode

Global Configuration mode

User Guidelines

If an IP address is not configured by this command, and no IP address is configured for the querier's VLAN, the querier is disabled.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 querier address 10.5.234.205
```

21.12. ip igmp snooping vlan querier election

To enable IGMP Querier election mechanism of an IGMP Snooping querier on a specific VLAN, use the `ip igmp snooping vlan querier election` command in Global Configuration mode. To disable Querier election mechanism, use the no form of this command.

Syntax

- ip igmp snooping vlan vlan-id querier election
- no ip igmp snooping vlan vlan-id querier election

Parameters

- vlan-id - Specifies the VLAN.

Default Configuration

Enabled

Command Mode

Global Configuration mode

User Guidelines

Use the no form of the ip igmp snooping vlan querier election command to disable IGMP Querier election mechanism on a VLAN.

If the IGMP Querier election mechanism is enabled, the IGMP Snooping querier supports the standard IGMP Querier election mechanism specified in RFC2236 and RFC3376.

If IGMP Querier election mechanism is disabled, IGMP Snooping Querier delays sending General Query messages for 60 seconds from the time it was enabled. During this time, if the switch did not receive an IGMP query from another Querier - it starts sending General Query messages. Once the switch acts as a Querier, it will stop sending General Query messages if it detects another Querier on the VLAN. In this case, the switch will resume sending General Query messages if it does hear another Querier for Query Passive interval that equals to

<Robustness>*<Query Interval> + 0.5*<Query Response Interval).

See the ip igmp robustness, ip igmp query-interval, and ip igmp query-max-response-time commands for configurations of these parameters.

It is recommended to disable IGMP Querier election mechanism if there is an IPM Multicast router on the VLAN.

Example

The following example disables IGMP Snooping Querier election on VLAN 1:

```
switchxxxxxx(config)# no ip igmp snooping vlan 1 querier election
```

21.13. ip igmp snooping vlan querier version

To configure the IGMP version of an IGMP Snooping querier on a specific VLAN, use the `ip igmp snooping vlan querier version` command in Global Configuration mode. To return to the default, use the no form of this command.

Syntax

- ip igmp snooping vlan vlan-id querier version {2 | 3}
- no ip igmp snooping vlan vlan-id querier version

Parameters

- vlan-id - Specifies the VLAN.
- querier version 2 - Specifies that the IGMP version would be IGMPv2.
- querier version 3 - Specifies that the IGMP version would be IGMPv3.

Default Configuration

IGMPv2.

Command Mode

Global Configuration mode

Example

The following example sets the version of the IGMP Snooping Querier VLAN 1 to 3:

```
switchxxxxxx(config)# ip igmp snooping vlan 1 querier version 3
```

21.14. ip igmp snooping vlan immediate-leave

To enable the IGMP Snooping Immediate-Leave processing on a VLAN, use the `ip igmp snooping vlan immediate-leave` Global Configuration mode command in Global Configuration mode. To return to the default, use the no form of this command.

Syntax

- ip igmp snooping vlan vlan-id immediate-leave
- no ip igmp snooping vlan vlan-id immediate-leave

Parameters

- vlan-id - Specifies the VLAN ID value. (Range: 1–4094).

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

You can execute the command before the VLAN is created.

Example

The following example enables IGMP snooping immediate-leave feature on VLAN.

```
switchxxxxxx(config)# ip igmp snooping vlan 1 immediate-leave
```

21.15. show ip igmp snooping cpe vlans

To display the CPE VLAN to Multicast TV VLAN mappings, use the `show ip igmp snooping cpe vlans` command in User EXEC mode.

Syntax

- show ip igmp snooping cpe vlans [vlan vlan-id]

Parameters

- vlan vlan-id - (Optional) Specifies the CPE VLAN ID.

Command Mode User EXEC mode Example

The following example displays the CPE VLAN to Multicast TV VLAN mappings.

```
switchxxxxxx# show ip igmp snooping cpe vlans
CPE VLAN Multicast-TV VLAN
-------- ------------------
2 1118
3 1119
```

21.16. show ip igmp snooping groups

To display the Multicast groups learned by the IGMP snooping, use the `show ip igmp snooping groups` command in User EXEC mode.

Syntax

- show ip igmp snooping groups [vlan vlan-id] [address ip-multicast-address] [source ip-address]

Parameters

- vlan vlan-id - (Optional) Specifies the VLAN ID.
- address ip-multicast-address - (Optional) Specifies the IP multicast address.
- source ip-address - (Optional) Specifies the IP source address.

Command Mode

User EXEC mode

User Guidelines

To see all Multicast groups learned by IGMP snooping, use the `show ip igmp snooping groups` command without parameters.

Use the `show ip igmp snooping groups` command with parameters to see a needed subset of all Multicast groups learned by IGMP snooping

To see the full Multicast address table (including static addresses), use the `show bridge multicast address-table` command.

Example

The following example shows sample output:

```
switchxxxxxx# show ip igmp snooping groups vlan 1
switchxxxxxx# show ip igmp snooping groups
Vlan Group Source Include Ports Exclude Ports Comp-Mode
 Address Address
---- ----------- ------- ------------ ------------ ---------
1     239.255.255.250 * te1/0/1 v2
```

21.17. show ip igmp snooping interface

To display the IGMP snooping configuration for a specific VLAN, use the `show ip igmp snooping interface` command in User EXEC mode.

Syntax

- show ip igmp snooping interface vlan-id

Parameters

- vlan-id - Specifies the VLAN ID.

Command Mode

User EXEC mode

Example

The following example displays the IGMP snooping configuration for VLAN 1000

```
switchxxxxxx# show ip igmp snooping interface 1000
IGMP Snooping is globally enabled
IGMP Snooping Querier is globally enabled
VLAN 1000
 IGMP Snooping is enabled
 IGMP snooping last immediate leave: enable
 Automatic learning of Multicast router ports is enabled
 IGMP Snooping Querier is enabled
 IGMP Snooping Querier operation state: is running
 IGMP Snooping Querier version: 2
 IGMP Snooping Querier election is enabled
 IGMP Snooping Querier address: 194.12.10.166
 IGMP snooping robustness: admin 2 oper 2
 IGMP snooping query interval: admin 125 sec oper 125 sec
 IGMP snooping query maximum response: admin 10 sec oper 10 sec
 IGMP snooping last member query counter: admin 2 oper 2
 IGMP snooping last member query interval: admin 1000 msec oper 500 msec Groups
that are in IGMP version 1 compatibility mode:
 231.2.2.3, 231.2.2.3
```

21.18. show ip igmp snooping mrouter

To display information on dynamically learned Multicast router interfaces for all VLANs or for a specific VLAN, use the `show ip igmp snooping mrouter` command in User EXEC mode.

Syntax

- show ip igmp snooping mrouter [interface vlan-id]

Parameters

- interface vlan-id - (Optional) Specifies the VLAN ID.

Command Mode

User EXEC mode

Example

The following example displays information on dynamically learned Multicast router interfaces for VLAN 1000:

```
switchxxxxxx# show ip igmp snooping mrouter interface 1000
VLAN Dynamic Static Forbidden
---- ------- ------ ---------
1000 te1/0/1 te1/0/2 te1/0/3-4
```

21.19. show ip igmp snooping multicast-tv

To display the IP addresses associated with Multicast TV VLANs, use the `show ip igmp snooping multicast-tv` EXEC mode command in User EXEC mode.

Syntax

- show ip igmp snooping multicast-tv [vlan vlan-id]

Parameters

- vlan vlan-id - (Optional) Specifies the VLAN ID.

Command Mode

User EXEC mode

Example

The following example displays the IP addresses associated with all Multicast TV VLANs.

```
switchxxxxxx# show ip igmp snooping multicast-tv
VLAN IP Address
---- ----------
1000 239.255.0.0
1000 239.255.0.1
1000 239.255.0.2
1000 239.255.0.3
1000 239.255.0.4
1000 239.255.0.5
1000 239.255.0.6
1000 239.255.0.7
```

22. IP Addressing Commands

Note:
IP addresses can be configured on the following Layer 2 interfaces:

- Ethernet port
- Port channel
- VLAN
- OOB port Lists of Commands

22.1. ip address

Use the `ip address` Interface Configuration (Ethernet, VLAN, Port-channel) mode command to define an IP address for an interface. Use the no form of this command to remove an IP address definition.

Syntax

OOB port:

- ip address ip-address {mask | /prefix-length} [default-gateway-ip-address]
- no ip address

In-Band interfaces:

- ip address ip-address {mask | /prefix-length}
- no ip address [ip-address]

Parameters

- ip-address - Specifies one of up to 32 IP addresses.
- mask - Specifies the network mask of the IP address.
- prefix-length - Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 8–30)
- default-gateway-ip-address - Specifies the default gateway IP address. The route is gotten a metric of 6 for an In-Band interface and 2 for OOB.

Default Configuration

No IP address is defined for interfaces.

Command Mode

Interface Configuration mode

User Guidelines

Use the `ip address` command to define a static IP address on an interface.

In-Band interfaces

Multiple IP addresses are supported. A new defined IP address is added on the interface.

Defining a static IP address on an interface stops a DHCP client running on the interface and removes the IP address assigned by the DHCP client.

If a configured IP address overlaps another configured one a warning message is displayed. To change an existed IP address, delete the existed one and add the new one.

OOB port

One IP address is supported. A new IP address defined on the OOB port overrides the previously defined IP address on the OOB port.

Defining a static IP address on the OOB port stops a DHCP client running on the OOB port and deletes an IP address assigned by the DHCP client.

While no IP address is assigned either by DHCP client or manually the default IP address 192.168.1.254 is assigned on the OOB port

Examples

Example 1. The following example configures VLAN 1 with IP address 131.108.1.27 and subnet mask 255.255.255.0.

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip address 131.108.1.27 255.255.255.0
```

Example 2. The following example configures 3 overlapped IP addresses.

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip address 1.1.1.1 255.0.0.0
switchxxxxxx(config)# exit
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# ip address 1.2.1.1 255.255.0.0
switchxxxxxx(config)# This IP address overlaps IP address 1.1.1.1/8 on vlan1,
are you sure? [Y/N]Y
switchxxxxxx(config)# exit
switchxxxxxx(config)# interface vlan 3
switchxxxxxx(config-if)# ip address 1.3.1.1 255.255.0.0
switchxxxxxx(config)# This IP address overlaps IP address 1.1.1.1/8 on vlan1,
are you sure? [Y/N]Y
switchxxxxxx(config)# exit
```

Example 3. The following example configures IP address on OOB:

```
switchxxxxxx(config)# interface oob
switchxxxxxx(config-if)# ip address 131.108.1.27 255.255.255.0 131.108.1.100
```

22.2. ip address dhcp

Use the `ip address dhcp` Interface Configuration (Ethernet, VLAN, Port-channel) mode command to acquire an IP address for an Ethernet interface from the Dynamic Host Configuration Protocol (DHCP) server. Use the no form of this command to release an acquired IP address.

Syntax

- ip address dhcp
- no ip address dhcp

Parameters

N/A

Command Mode

Interface Configuration mode

User Guidelines

Use the `ip address dhcp` command to enable DHCP client on the interface.

The ip address dhcp command removes all the manually configured addresses on the interface.

The default route (Default Gateway) received in DHCP Router option (Option 3) is assigned a metric of 8 for an In-Band interface and 4 for OOB.

Use the no form of the command to disable DHCP client on interface.

Example

The following example acquires an IP address for VLAN 100 from DHCP.

```
switchxxxxxx(config)# interface vlan100
switchxxxxxx(config-if)# ip address dhcp
```

22.3. renew dhcp

Use the `renew dhcp` Privileged EXEC mode command to renew an IP address that was acquired from a DHCP server for a specific interface.

Syntax

- renew dhcp interface-id [force-autoconfig]

Parameters

- interface-id - Specifies an interface.
- force-autoconfig - If the DHCP server holds a DHCP option 67 record for the assigned IP address, the record overwrites the existing device configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Use the `renew dhcp` command to renew a DHCP address on an interface.

This command does not enable DHCP client on an interface and if DHCP client is not enabled on the interface, the command returns an error message.

Example

The following example renews an IP address on VLAN 19 that was acquired from a DHCP server:

```
switchxxxxxx# renew dhcp vlan 19
```

22.4. ip default-gateway

The `ip default-gateway` Global Configuration mode command defines a default gateway (device). Use the no form of this command to restore the default configuration.

Syntax

- ip default-gateway ip-address
- no ip default-gateway [ip-address]

Parameters

- ip-address - Specifies the default gateway IP address.

Command Mode

Global Configuration mode

Default Configuration

No default gateway is defined.

User Guidelines

Use the `ip default-gateway` command to defines a default gateway (default route).

The ip default-gateway command adds the default route with metric of 6 for the gateway connected on an In-Band interface and 2 for the gateway connected on OOB.

Use the no ip default-gateway ip-address command to delete one default gateway.

Use the no ip default-gateway command to delete all default gateways.

Example

The following example defines default gateway 192.168.1.1.

```
switchxxxxxx(config)# ip default-gateway 192.168.1.1
```

22.5. show ip interface

Use the `show ip interface` EXEC mode command to display the usability status of configured IP interfaces.

Syntax

- show ip interface [interface-id]

Parameters

- interface-id - Specifies an interface ID on which IP addresses are defined.

Default Configuration

All IP addresses.

Command Mode

User EXEC mode

Examples

Example 1 - The following example displays all configured IP addresses and their types:

```
switchxxxxxx# show ip interface
!source_precedence_is_supported &&
!broadcast_address_configuration_is_supported && ip_redirects_is_supported
IP Address I/F I/F Status Type Directed Redirect Status
 admin/oper Broadcast
-------------- ------ ----------- ------- -------- --------- -----
10.5.230.232/24 vlan 1 UP/UP Static disable Enabled Valid
10.5.234.202/24 vlan 4 UP/DOWN Static disable Disabled Valid
10.5.240.200/24 oob UP/UP Static Valid
```

Example 2 - The following example displays the IP addresses configured on the given L2 interfaces and their types:

```
switchxxxxxx# show ip interface vlan 1
!source_precedence_is_supported &&
!broadcast_address_configuration_is_supported && ip_redirects_is_supported
IP Address I/F I/F Status Type Directed Redirect Status
 admin/oper Broadcast
```

```
------------ ------ ----------- ------- -------- --------- -----
10.5.230.232/24 vlan 1 UP/UP Static disable Enabled Valid
```

22.6. arp

Use the `arp` Global Configuration mode command to add a permanent entry to the Address Resolution Protocol (ARP) cache. Use the no form of this command to remove an entry from the ARP cache.

Syntax

- arp ip-address mac-address [interface-id]
- no arp ip-address

Parameters

- ip-address - IP address or IP alias to map to the specified MAC address.
- mac-address - MAC address to map to the specified IP address or IP alias.
- interface-id - Address pair is added for specified interface.

Command Mode

Global Configuration mode

Default Configuration

No permanent entry is defined.

If no interface ID is entered, address pair is relevant to all interfaces.

User Guidelines

The software uses ARP cache entries (up to 1024) to translate 32-bit IP addresses into 48-bit hardware (MAC) addresses. Because most hosts support dynamic address resolution, static ARP cache entries generally do not need to be specified.

Example

The following example adds IP address 198.133.219.232 and MAC address 00:00:0c:40:0f:bc to the ARP table.

```
switchxxxxxx(config)# arp 198.133.219.232 00:00:0c:40:0f:bc vlan100
```

22.7. arp timeout (Global)

Use the `arp timeout` Global Configuration mode command to set the time interval during which an entry remains in the ARP cache. Use the no form of this command to restore the default configuration.

Syntax

- arp timeout seconds
- no arp timeout

Parameters

- seconds - Specifies the time interval (in seconds) during which an entry remains in the ARP cache. (Range: 1–40000000).

Default Configuration

The default ARP timeout is 60000 seconds, if IP Routing is enabled, and 300 seconds if IP Routing is disabled.

Command Mode

Global Configuration mode

Example

The following example configures the ARP timeout to 12000 seconds.

```
switchxxxxxx(config)# arp timeout 12000
```

22.8. ip arp proxy disable

Use the `ip arp proxy disable` Global Configuration mode command to globally disable proxy Address Resolution Protocol (ARP). Use the no form of this command reenable proxy ARP.

Syntax

- ip arp proxy disable
- no ip arp proxy disable

Parameters

N/A

Default

Enabled by default.

Command Mode

Global Configuration mode

User Guidelines

This command overrides any proxy ARP interface configuration.

The command is supported only when IP Routing is enabled.

Example

The following example globally disables ARP proxy.

```
switchxxxxxx(config)# ip arp proxy disable
```

22.9. ip proxy-arp

Use the `ip proxy-arp` Interface Configuration mode command to enable an ARP proxy on specific interfaces. Use the no form of this command disable it.

Syntax

- ip proxy-arp
- no ip proxy-arp

Default Configuration

ARP Proxy is disabled.

Command Mode

Interface Configuration mode

User Guidelines

This configuration can be applied only if at least one IP address is defined on a specific interface.

The command is supported only when IP Routing is enabled.

Example

The following example enables ARP proxy when the switch is in router mode.

```
switchxxxxxx(config-if)# ip proxy-arp
```

22.10. clear arp-cache

Use `the clear arp-cache` Privileged EXEC mode command to delete all dynamic entries from the ARP cache.

Syntax

- clear arp-cache

Command Mode

Privileged EXEC mode

Example

The following example deletes all dynamic entries from the ARP cache.

```
switchxxxxxx# clear arp-cache
```

22.11. show arp

Use the `show arp` Privileged EXEC mode command to display entries in the ARP table.

Syntax

- show arp [ip-address ip-address] [mac-address mac-address] [interface-id]

Parameters

- ip-address ip-address - Specifies the IP address.
- mac-address mac-address - Specifies the MAC address.
- interface-id - Specifies an interface ID.

Command Mode

Privileged EXEC mode

User Guidelines

Since the associated interface of a MAC address can be aged out from the FDB table, the Interface field can be empty.

If an ARP entry is associated with an IP interface that is defined on a port or port-channel, the VLAN field is empty.

Example

The following example displays entries in the ARP table.

```
switchxxxxxx# show arp
ARP timeout: 80000 Seconds
VLAN Interface IP Address HW Address Status
```

```
------- --------- ---------- ---------- ------
VLAN 1 te1/0/1 10.7.1.102 00:10:B5:04:DB:4B Dynamic
VLAN 1 te1/0/2 10.7.1.135 00:50:22:00:2A:A4 Static
VLAN 2 te1/0/1 11.7.1.135 00:12:22:00:2A:A4 Dynamic
 te1/0/2 12.10.1.13 00:11:55:04:DB:4B Dynamic
```

22.12. show arp configuration

Use the `show arp configuration` privileged EXEC command to display the global and interface configuration of the ARP protocol.

Syntax

- show arp configuration

Parameters

This command has no arguments or key words.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show arp configuration
Global configuration:
ARP Proxy: enabled
ARP timeout: 80000 Seconds
Interface configuration:
VLAN 1:
ARP Proxy: disabled
ARP timeout:60000 Seconds
VLAN 10:
ARP Proxy: enabled
ARP timeout:70000 Seconds
VLAN 20:
ARP Proxy: enabled
ARP timeout:80000 Second (Global)
```

22.13. interface ip

Use the `interface ip` Global Configuration mode command to enter the IP Interface Configuration mode.

Syntax

- interface ip ip-address

Parameters

- ip-address - Specifies one of the IP addresses of the device.

Command Mode

Global Configuration mode

Example

The following example enters the IP interface configuration mode.

```
switchxxxxxx(config)# interface ip 192.168.1.1
switchxxxxxx(config-ip)#
```

22.14. ip helper-address

Use the `ip helper-address` Global Configuration mode command to enable the forwarding of UDP Broadcast packets received on an interface to a specific (helper) address. Use the no form of this command to disable the forwarding of broadcast packets to a specific (helper) address.

Syntax

- ip helper-address {ip-interface | all} address [udp-port-list]
- no ip helper-address {ip-interface | all} address

Parameters

- ip-interface - Specifies the IP interface.
- all - Specifies all IP interfaces.
- address - Specifies the destination broadcast or host address to which to forward UDP broadcast packets. A value of 0.0.0.0 specifies that UDP broadcast packets are not forwarded to any host.
- udp-port-list - Specifies the destination UDP port number to which to forward Broadcast packets. (Range: 1–65535). This can be a list of port numbers separated by spaces.

Default Configuration

Forwarding of UDP Broadcast packets received on an interface to a specific (helper) address is disabled.

If udp-port-list is not specified, packets for the default services are forwarded to the helper address.

Command Mode

Global Configuration mode

User Guidelines

This command forwards specific UDP Broadcast packets from one interface to another, by specifying a UDP port number to which UDP broadcast packets with that destination port number are forwarded. By default, if no UDP port number is specified, the device forwards UDP broadcast packets for the following six services:

- IEN-116 Name Service (port 42)
- DNS (port 53)
- NetBIOS Name Server (port 137)
- NetBIOS Datagram Server (port 138)
- TACACS Server (port 49)
- Time Service (port 37)

Many helper addresses may be defined. However, the total number of address-port pairs is limited to 128 for the device.

The setting of a helper address for a specific interface has precedence over the setting of a helper address for all the interfaces.

Forwarding of BOOTP/DHCP (ports 67, 68) cannot be enabled with this command. Use the DHCP relay commands to relay BOOTP/DHCP packets.

The ip-interface argument cannot be the OOB port.

Example

The following example enables the forwarding of UDP Broadcast packets received on all interfaces to the UDP ports of a destination IP address and UDP port 1 and 2.

```
switchxxxxxx(config)# ip helper-address all 172.16.9.9 49 53 1 2
```

22.15. show ip helper-address

Use the `show ip helper-address` Privileged EXEC mode command to display the IP helper addresses configuration on the system.

Syntax

- show ip helper-address

Parameters

This command has no arguments or key words.

Command Mode

Privileged EXEC mode

User Guidelines

Example

The following example displays the IP helper addresses configuration on the system:

```
switchxxxxxx# show ip
      Interface   Helper Address    UDP Ports
      ------------      --------------    ------------------------
      192.168.172.16.37, 42, 49, 53, 137, 138
      192.168.172.16.37, 49
```

22.16. show ip dhcp client interface

Use the `show ip dhcp client interface` command in User EXEC or Privileged EXEC mode to display DHCP client interface information.

Syntax

- show ip dhcp client interface [interface-id]

Parameters

- interface-id - Interface identifier.

Command Mode

User EXEC mode

User Guidelines

If no interfaces are specified, all interfaces on which DHCP client is enabled are displayed. If an interface is specified, only information about the specified interface is displayed.

Example

The following is sample output of the show ip dhcp client interface command:

```
switchxxxxxx# show ip dhcp client interface
```

```
VLAN 100 is in client mode
 Address: 170.10.100.100 Mask: 255.255.255.0 T1 120, T2 192
 Default Gateway: 170.10.100.1
 DNS Servers: 115.1.1.1, 87.12.34.20
 DNS Domain Search List: company.com
 Host Name: switch_floor7
 Configuration Server Addresses: 192.1.1.1 202.1.1.1
 Configuration Path Name: qqq/config/aaa_config.dat
 Image Path Name: qqq/image/aaa_image.ros
 POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
VLAN 1200 is in client mode
 Address: 180.10.100.100 Mask: 255.255.255.0 T1 120, T2 192
 Default Gateway: 180.10.100.1
 DNS Servers: 115.1.1.1, 87.12.34.20
 DNS Domain Search List: company.com
 Host Name: switch_floor7
 Configuration Server Addresses: configuration.company.com
 Configuration Path Name: qqq/config/aaa_config.dat
 Image Path Name: qqq/image/aaa_image.ros
 POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
```

23. IP Routing Protocol-Independent Commands

23.1. accept-lifetime

To set the time period during which the authentication key on a key chain is received as valid, use the `accept-lifetime` command inkey chain key configuration mode. To revert to the default value, use the no form of this command.

Syntax

- accept-lifetime start-time {infinite | end-time | duration seconds}
- no accept-lifetime

Parameters

- start-time - Beginning time that the key specified by the key command is valid to be received. The Syntax can be either of the following:
  - hh:mm:ss Month date year
  - hh:mm:ss date Month year
  - hh - hours (0-23)
  - mm - minutes (0-59)
  - ss - seconds (0-59)
  - Month - first three letters of the month
  - date - date (1-31)
  - year - year (four digits)

The default start time and the earliest acceptable date is January 1, 2000.

- infinite - Key is valid to be received from the start-time value on.
- end-time - Key is valid to be received from the start-time value until the end-time value. The Syntax is the same as that for the start-time value. The end-time value must be after the start-time value. The default end time is an infinite time period.
- duration seconds - Length of time (in seconds) that the key is valid to be received. The range is from 1 to 2147483646.

Default Configuration

The default time period during which the authentication key is valid for authenticating incoming packets is set to Forever.

The definition of Forever is: the starting time is January 1, 2000, and the ending time is infinite.

Command Mode

Key Chain Key Configuration mode

User Guidelines

The switch checks Time-of-Date again a value of the start-time argument regardless if Time-of-Date is not set by management or by SNTP because of the default value of Time-of-Date always is an passed time.

If validation of the value of the start-time argument was passed and the end-time argument is configured and its value is infinite the key is considered as actual regardless if Time-of-Date is not set by management or by SNTP.

If Time-of-Date is not set by management or by SNTP and if the end-time argument is configured with a value differing from infinite or the duration parameter is configured, the key is considered as expired.

If Time-of-Date is set by management or by SNTP, the switch checks Time-of-Date again a value of the end-time argument or of the duration parameter.

If the last key expires, authentication will be finished with error.

Example

The following example configures a key chain called keychain1. The key named string1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named string2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or discrepancies in the set time of the router. There is a 30-minute leeway on each side to handle time differences:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 172.19.1.1
switchxxxxxx(config-rip)# exit
switchxxxxxx(config)# interface ip 172.19.1.1
switchxxxxxx(config-ip)# ip rip authentication mode md5
switchxxxxxx(config-ip)# ip rip authentication key-chain keychain1
switchxxxxxx(config-ip)# exit
switchxxxxxx(config)# key chain keychain1
switchxxxxxx(config-keychain)# key 1
switchxxxxxx(config-keychain-key)# key-string string1
switchxxxxxx(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2011 duration
7200
switchxxxxxx(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2011 duration
3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# key 2
switchxxxxxx(config-keychain-key)# key-string string2
switchxxxxxx(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2011 duration
7200
switchxxxxxx(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2011 duration
3600
switchxxxxxx(config-keychain-key)# exit
```

23.2. directed-broadcast

Use the `directed-broadcast` IP Interface Configuration mode command to enable the translation of a directed broadcast to physical broadcasts. Use the no form of this command to disable this function.

Syntax

- directed-broadcast
- no directed-broadcast

Default Configuration

Translation of a directed broadcast to physical broadcasts is disabled. All IP directed broadcasts are dropped.

Command Mode

IP Configuration mode

Example

The following example enables the translation of a directed broadcast to physical broadcasts.

```
switchxxxxxx(config)# interface ip 192.168.1.1
switchxxxxxx(config-ip)# directed-broadcast
```

23.3. ip redirects

Use the `ip redirects` command in IP Interface Configuration mode to enable the sending of ICMP redirect messages to re-send a packet through the same interface on which the packet was received. To disable the sending of redirect messages, use the no form of this command.

Syntax

- ip redirects
- no ip redirects

Parameters

N/A.

Default Configuration

The sending of ICMP redirect messages is enabled.

Command Mode

IP Configuration mode

Example

The following example disables the sending of ICMP redirect messages on IP interface 1.1.1.1 and re-enables the messages on IP interface 2.2.2.2:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# no ip redirects
switchxxxxxx(config-ip)# exit
switchxxxxxx(config)# interface ip 2.2.2.2
switchxxxxxx(config-ip)# ip redirects
switchxxxxxx(config-ip)# exit
```

23.4. ip route

To establish up to 124 static routes, use the `ip route` command in global configuration mode. To remove static routes, use the no form of this command.

Syntax

- ip route prefix {mask | /prefix-length} {{ip-address [metric value]} | reject-route}
- no ip route prefix {mask | /prefix-length} [ip-address]

Parameters

- prefix - IP route prefix for the destination.
- mask - Prefix mask for the destination.
- /prefix-length - Prefix mask for the destination.Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0–32)
- ip-address - IP address of the next hop that can be used to reach that network.

- metric value - Metric of the route. The default metric is 6 for the Next Hop on an In-Band interface and 2 for the Next Hop on OOB. Range: 1–255.
- reject-route - Stopping routing to the destination network.

Default Configuration

No static routes are established.

Command Mode

Global Configuration mode

User Guidelines

Use the `no ip route` command without the ip-address parameter to remove all static routes to the given subnet.

Use the `no ip route` command with the ip-address parameter to remove only one static route to the given subnet via the given next hop.

Examples

Example 1 - The following example shows how to route packets for network 172.31.0.0 to a router at 172.31.6.6 using mask:

```
switchxxxxxx(config)# ip route 172.31.0.0 255.255.0.0 172.31.6.6 metric 2
```

Example 2 - The following example shows how to route packets for network 172.31.0.0 to a router at 172.31.6.6 using prefix length :

```
switchxxxxxx(config)# ip route 172.31.0.0 /16 172.31.6.6 metric 2
```

Example 3 - The following example shows how to reject packets for network 194.1.1.0:

```
switchxxxxxx(config)# ip route 194.1.1.0 255.255.255.0 reject-route
```

Example 4 - The following example shows how to remove all static routes to network 194.1.1.0/24:

```
switchxxxxxx(config)# no ip route 194.1.1.0 /24
```

Example 5 - The following example shows how to remove one static route to network 194.1.1.0/24 via 1.1.1.1:

```
switchxxxxxx(config)# no ip route 194.1.1.0 /24 1.1.1.1
```

23.5. ip routing

To enable IP routing, use the `ip routing` command in global configuration mode. To disable IP routing, use the no form of this command.

Syntax

- ip routing
- no ip routing

Parameters

This command has no arguments or keywords.

Default Configuration

IP routing is enabled.

Command Mode

Global Configuration mode

User Guidelines

Use the command to enable IP Routing.

The switch supports one IPv4 stack on in-band interfaces and the OOB port.

The IP stack is always running on the OOB port as an IP host regardless whether IP routing is enabled.

The switch blocks routing between in-band interfaces and the OOB interface.

In the case when there are two best routes - one via an in-band and one via the OOB port, the switch will use the route via the OOB port.

DHCP Relay and IP Helper cannot be enabled on the OOB port.

Routing protocols cannot be enabled on the OOB port.

The IP subnet defined on the OOB port is not redistributed to routing protocols running on in-band interfaces.

Note:
The IPv6 routing is disabled by default.

Example

The following example enables IP routing

```
switchxxxxxx(config)# ip routing
```

23.6. key-string

To specify the authentication string for a key, use the `key-string` command in key chain key configuration mode. To remove the authentication string, use the no form of this command.

Syntax

- key-string text
- no key-string

Parameters

- text - Specifies the authentication string. The string can contain from 1 to 16 characters.

Default Configuration

No key exists.

Command Mode

Key Chain Key Configuration mode

Example

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences:

```
switchxxxxxx(config)# key chain chain1
switchxxxxxx(config-keychain)# key 1
switchxxxxxx(config-keychain-key)# key-string key1
switchxxxxxx(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2011 duration
7200
switchxxxxxx(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2011 duration
3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# key 2
switchxxxxxx(config-keychain-key)# key-string key2
switchxxxxxx(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2011 duration
7200
switchxxxxxx(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2011 duration
3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# exit
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 172.19.1.1
switchxxxxxx(config-rip)# version 2
switchxxxxxx(config-rip)# exit
switchxxxxxx(config)# interface ip 172.19.1.1
switchxxxxxx(config-ip)# ip rip authentication key-chain chain1
switchxxxxxx(config-ip)# ip rip authentication mode md5
switchxxxxxx(config-ip)# exit
```

23.7. key (key chain)

To identify an authentication key on a key chain, use the `key` command in key-chain configuration mode. To remove the key from the key chain, use the no form of this command.

Syntax

- key key-id
- no key key-id

Parameters

- key-id - Identification number of an authentication key on a key chain. The range of keys is from 1 to 255. The key identification numbers need not be consecutive. The scope of a key identification number is the key chain where the key is defined.

Default Configuration

No key exists on the key chain.

Command Mode

Key-Chain Configuration mode

User Guidelines

It is useful to have multiple keys on a key chain so that the software can sequence through the keys as they become invalid after time, based on the accept-lifetime and send-lifetime key chain key command settings.

Each key has its own key identifier, which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and authentication key in use. Only one authentication packet is sent, regardless of the number of valid keys. The software starts looking at the lowest key identifier number and uses the first valid key.

If the last key expires, authentication will be finished with error.

To remove all keys, remove the key chain by using the no key chain command.

Example

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences:

```
switchxxxxxx(config)# key 1
switchxxxxxx(config)# key chain chain1
switchxxxxxx(config-keychain)# key 1
switchxxxxxx(config-keychain-key)# key-string key1
switchxxxxxx(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2011 duration
7200
switchxxxxxx(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2011 duration
3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# key 2
switchxxxxxx(config-keychain-key)# key-string key2
switchxxxxxx(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2011 duration
7200
switchxxxxxx(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2011 duration
3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# exit
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 172.19.1.1 exit
switchxxxxxx(config)# interface ip 172.19.1.1
switchxxxxxx(config-ip)# ip rip authentication mode md5
switchxxxxxx(config-ip)# ip rip authentication key-chain chain1
switchxxxxxx(config-ip)# exit
```

23.8. key chain

To enable authentication for routing protocols, identify a group of authentication keys by using the key chain command in global configuration mode. To remove the key chain, use the no form of this command

Syntax

- key chain name-of-chain
- no key chain name-of-chain

Parameters

- name-of-chain - Name of a key chain. The chain-name may have from 1 to 32 characters. A key chain must have at least one key and can have up to 256 keys.

Default Configuration

No key chain exists.

Command Mode

Global Configuration mode

User Guidelines

You must configure a key chain with keys to enable authentication.

Although you can identify multiple key chains, we recommend using one key chain per interface per routing protocol. Upon specifying the key chain command, you enter key-chain configuration mode.

Example

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences:

```
switchxxxxxx(config)# key chain chain1
switchxxxxxx(config-keychain)# key 1
switchxxxxxx(config-keychain-key)# key-string key1
switchxxxxxx(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2011 duration
7200
switchxxxxxx(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2011 duration
3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# key 2
switchxxxxxx(config-keychain-key)# key-string key2
switchxxxxxx(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2011 duration
7200
switchxxxxxx(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2011 duration
3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# exit
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 172.19.1.1
switchxxxxxx(config-rip)# exit
switchxxxxxx(config)# interface ip 172.19.1.1
switchxxxxxx(config-ip)# ip rip authentication mode md5
switchxxxxxx(config-ip)# ip rip authentication key-chain chain1
switchxxxxxx(config-ip)# exit
```

23.9. send-lifetime

To set the time period during which an authentication key on a key chain is valid to be sent, use the `send-lifetime` command in Key Chain Key configuration mode. To revert to the default value, use the no form of this command.

Syntax

- send-lifetime start-time {infinite | end-time | duration seconds}
- no send-lifetime

Parameters

- start-time - Beginning time that the key specified by the key command is valid to be received. The Syntax can be either of the following:
  - hh:mm:ss Month date year
  - hh:mm:ss date Month year
  - hh - hours (0-23)

- mm - minutes (0-59)
- ss - seconds (0-59)
- Month - first three letters of the month
- date - date (1-31)
- year - year (four digits)

The default start time and the earliest acceptable date is January 1, 2000.

- infinite - Key is valid to be received from the start-time value on.
- end-time - Key is valid to be received from the start-time value until the end-time value. The Syntaxis the same as that for the start-time value. The end-time value must be after the start-time value. The default end time is an infinite time period.
- duration seconds - Length of time (in seconds) that the key is valid to be received. The range is from 1 to 2147483646.

Default Configuration

The default time period during which the authentication key is valid for authenticating incoming packets is set to forever.

Forever (the starting time is January 1, 2000, and the ending time is infinite)

Command Mode

Key Chain Key Configuration mode

User Guidelines

Specify a start-time value and one of the following values: infinite end-time, or duration seconds.

A key is considered as expired if Time-of-Date is not set by management or by SNTP.

If the last key expires, authentication will be finished with error.

Example

The following example configures a key chain called chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from

3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or discrepancies in the set time of the router. There is a 30-minute leeway on each side to handle time differences:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 172.19.1.1
switchxxxxxx(config-rip)# exit
switchxxxxxx(config)# interface ip 172.19.1.1
switchxxxxxx(config-ip)# ip rip authentication mode md5
switchxxxxxx(config-ip)# ip rip authentication key-chain chain1
switchxxxxxx(config-ip)# exit
switchxxxxxx(config)# key chain chain1
switchxxxxxx(config-keychain)# key 1
switchxxxxxx(config-keychain-key)# key-string key1
switchxxxxxx(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration
7200
switchxxxxxx(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration
3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# key 2
switchxxxxxx(config-keychain-key)# key-string key2
```

```
switchxxxxxx(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration
7200
switchxxxxxx(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration
3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# exit
```

23.10. show ip protocols

To display the parameters and current state of the active IP routing protocol processes, use the `show ip protocols` command in user EXEC or privileged EXEC mode.

Syntax

- show ip protocols [summary]

Parameters

- summary - Displays the configured routing protocol process names.

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

The information displayed by the show ip protocols command is useful in debugging routing operations.

Examples

Example 1. The following is sample output from the show ip protocols command, showing active routing protocols:

```
switchxxxxxx# show ip protocols
IP Routing Protocol is "rip"
 Interfaces IP Addresses
 VLAN 1 12.1.1.1
 VLAN 1 150.23.12.2
 VLAN 11 1.1.1.1
IP Routing Protocol is "ospf 1"
 Interfaces IP Addresses
 VLAN 3 2.2.2.2
 VLAN 100 154.23.111.1
IPv6 Routing Protocol is "ospf 10"
 Interfaces IP Addresses
 VLAN 10 123.1.1.1
 VLAN 130 4.4.4.4
```

Example 2. The following is sample output from the show ip protocols command with the summary keyword:

```
switchxxxxxx# show ipv6 protocols summary
IP Routing Protocol is "rip"
IP Routing Protocol is "ospf 1"
IP Routing Protocol is "ospf 10"
```

23.11. show ip route

To display the current state of the routing table, use the `show ip route` command in user EXEC or privileged EXEC mode.

Syntax

- show ip route [address ip-address {mask [longer-prefixes]} [protocol [process-id] | static | rejected | icmp | connected]

Parameters

- address ip-address - IP address about which routing information should be displayed.
- mask - The value of the subnet mask.
- longer-prefixes - Specifies that only routes matching the IP address and mask pair should be displayed.
- protocol - The name of the origin of the protocol to be displayed. Use one of the following arguments:
  - rip - Displays routes added by RIP
  - ospf process-id - Displays routes added by OSPF. process_id is the number used to identify a specific process of OSPF.
- connected - Displays connected routes.
- icmp - Displays routes added by ICMP Direct.
- rejected - Displays rejected routes.
- static - Displays static routes.

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

Use this command without parameters to display the whole IPv6 Routing table.

Use this command with parameters to specify required routes.

Examples

Example 1. The following is sample output from the show ip route command when IP Routing is not enabled:

```
switchxxxxxx# show ip route
Maximum Parallel Paths: 1 (1 after reset)
IP Forwarding: disabled
Codes: > - best, C - connected, S - static, I - ICMP
IP Routing Table - 5 entries
Code IP Route Distance/ Next Hop Last Time Outgoing
  Metric IP Address Updated Interface
------ ------------------ ----------- --------------- ------------ -----------
-
S 10.10.0.0/16 1/2 10.119.254.244 00:02:22 vlan2
S> 10.10.0.0/16 1/1 10.120.254.244 00:02:22 vlan3
S> 10.16.2.0/24 1/1 10.119.254.244 00:02:22 vlan2 C> 10.119.0.0/16 0/1 0.0.0.0
vlan2
C> 10.120.0.0/16 0/1 0.0.0.0  vlan3
```

Example 2. The following is sample output from the show ip route command when IP Routing is enabled:

```
switchxxxxxx# show ip route
Maximum Parallel Paths: 1 (1 after reset)
IP Forwarding: enabled
Directed Broadcast Forwarding: disabled
Codes: > - best, C - connected, S - static Codes: > - best, C - connected, S -
static
 R - RIP
 O - OSPF intra-area, OIA - OSPF inter-area, OE1 - OSPF external 1, OE2 - OSPF
external 2
IP Routing Table - 23 entries
Code IP Route Distance/ Next Hop Last Time Outgoing
  Metric IP Address Updated Interface
------ ------------------ ----------- --------------- ------------ -----------
-
R> 10.7.10.0/24 120/5 10.119.254.244 00:02:22 vlan2
O> 10.10.0.0/16 10/128 10.119.254.244 00:02:22 vlan2
O> 10.10.0.0/16 10/128 10.120.254.244 00:02:22 vlan3
O> 10.16.2.0/24 110/128 10.119.254.244 00:02:22 vlan2
O> 10.16.2.64/26 110/128 10.119.254.244 00:02:22 vlan2
O> 10.16.2.64/26 110/130 10.119.254.244 00:02:22 vlan3
O> 10.16.2.128/26 110/128 10.119.254.244 00:02:22 vlan2
O> 10.16.208.0/24 110/128 10.120.254.244 00:02:22 vlan2
O> 10.16.223.0/24 110/128 10.119.254.244 00:02:22 vlan2
O> 10.16.236.0/24 110/129 10.119.254.240 00:02:23 vlan2
OE2> 10.68.132.0/24 110/5 10.119.254.6 00:00:59 vlan2
O> 10.75.139.0/24 110/129 10.119.254.240 00:02:23 vlan2
O> 10.84.148.0/24 110/129 10.119.254.240 00:02:23 vlan2
OE2 > 10.110.0.0/24 110/128 10.119.254.6 00:01:00 vlan1
O> 10.128.0.0/16 110/128 10.119.254.244 00:02:22 vlan2
O> 10.129.0.0/16 110/129 10.119.254.240 00:02:02 vlan2 OE2> 10.130.0.0/16 110/5
0.0.0.0 00:00:59 vlan2
O> 10.140.0.0/16 110/129 10.119.254.240 00:02:23 vlan2 O> 10.141.0.0/16 110/129
10.119.254.240 00:02:22 vlan2
S> 10.175.0.0/16 1/1 10.119.254.240 00:02:22 vlan2 S> 10.180.0.0/16 1/1
10.119.254.240 00:02:42 vlan3
C> 10.119.0.0/16 0/1 0.0.0.0  vlan2
C> 10.120.0.0/16 0/1 0.0.0.0  vlan3
```

Example 3. In the following example, the logical AND operation is performed on the address 10.16.0.0 and the mask 255.255.0.0, resulting in 10.16.0.0. On each destination in the routing table the logical AND operation is also performed with the mask and the result is compared with 10.16.0.0. Any destinations that fall into that range are displayed in the output:

```
switchxxxxxx# show ip route 10.16.0.0 255.255.0.0 longer-prefix
Maximum Parallel Paths: 1 (1 after reset)
IP Forwarding: enabled
Directed Broadcast Forwarding: disabled
Codes: > - best, C - connected, S - static
 R - RIP
 O - OSPF intra-area, OIA - OSPF inter-area, OE1 - OSPF external 1, OE2 - OSPF
external 2
IP Routing Table - 6 entries
Code IP Route Distance/ Next Hop Last Time Outgoing
```

```
  Metric IP Address Updated Interface
------ ------------------ ---------- -------------- ------------ -----------
-
S> 10.16.2.0/24 1/1 10.119.254.244 00:02:22 vlan2
S> 10.16.2.64/26 1/1 100.1.14.244 00:02:22 vlan1
S> 10.16.2.128/26 1/1 110.9.2.2 00:02:22 vlan3
S> 10.16.208.0/24 1/1 120.120.5.44 00:02:22 vlan2
S> 10.16.223.0/24 1/1 20.1.2.24 00:02:22 vlan5
S> 10.16.236.0/24 1/1 30.19.54.240 00:02:23 vlan6 C> 10.119.0.0/16 0/1 0.0.0.0
vlan2
C> 10.120.0.0/16 0/1 0.0.0.0  vlan3
C> 20.1.0.0/16 0/1 0.0.0.0  vlan5
C> 30.19.0.0/16 0/1 0.0.0.0  vlan2
C> 100.1.0.0/16 0/1 0.0.0.0  vlan1
C> 110.9.0.0/16 0/1 0.0.0.0  vlan3
C> 120.120.0.0/16 0/1 0.0.0.0  vlan2
```

23.12. show ip route summary

Use the `show ip route summary` command in User EXEC or Privileged EXEC mode to display the current contents of the IP routing table in summary format.

Syntax

- show ip route summary

Parameters

N/A.

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

Example

The following is sample output from the show ip route summary command:

```
switchxxxxxx# show ip route summary
IP Routing Table Summary - 90 entries
35 connected, 25 static, 12 RIP, 10 OSPF Number of prefixes:
/16: 16, /18: 10, /22: 15, /24: 25, /28: 2, /30: 6
```

23.13. show key chain

To display authentication key information, use the `show key chain` command in Privileged EXEC mode.

Syntax

- show key chain [name-of-chain]

Parameters

- name-of-chain - Name of the key chain to display, as named in the key chain command.

Default Configuration

Information about all key chains is displayed.

Command Mode

Privileged EXEC mode

User Guidelines

Examples

Example 1. The following is sample output from the show key chain command when the current time od date is defined:

```
switchxxxxxx# show key chain
Current Time of Date is Feb 8 2011 Accept lifetime is configured to ignore
Key-chain trees:
 key 1 -- text "chestnut" accept lifetime (always valid) - (always valid) [valid
now] send lifetime (always valid) - (always valid) [valid now] key 2 -- text
"birch" accept lifetime (00:00:00 Dec 5 2010) - (23:59:59 Dec 5 2010) send
lifetime (06:00:00 Dec 5 2010) - (18:00:00 Dec 5 2016)[valid now]
```

Example 2. The following is sample output from the show key chain command when the current time od date is not defined:

```
switchxxxxxx# show key chain
Current Time of Date is not defined
Accept lifetime is ignored Key-chain trees:
 key 1 -- text "chestnut" accept lifetime (always valid) - (always valid) [valid
now] send lifetime (always valid) - (always valid) [valid now] key 2 -- text
"birch" accept lifetime (00:00:00 Dec 5 2010) - (23:59:59 Dec 5 2010) send
lifetime (06:00:00 Dec 5 2010) - (18:00:00 Dec 5 2016)
```

24. IP System Management Commands

24.1. ping

Use the `ping` EXEC mode command to send ICMP echo request packets to another node on the network.

Syntax

- ping [ip] {ipv4-address | hostname} [size packet_size] [count packet_count] [timeout time_out] [source source-address]
- ping ipv6 {ipv6-address | hostname} [size packet_size] [count packet_count] [timeout time_out] [source source-address]

Parameters

- ip - Use IPv4 to check the network connectivity.
- ipv6 - Use IPv6 to check the network connectivity.
- ipv4-address - IPv4 address to ping.
- ipv6-address - Unicast or Multicast IPv6 address to ping. When the IPv6 address is a Link Local address (IPv6 address), the outgoing interface name must be specified.
- hostname - Hostname to ping (Length: 1-158 characters. Maximum label size for each part of the host name: 58.)
- size packet_size - Number of bytes in the packet not including the VLAN tag. The default is 64 bytes. (IPv4:64–1518, IPv6: 68–1518)
- count packet_count - Number of packets to send, from 1 to 65535 packets. The default is 4 packets. If 0 is entered, it pings until stopped (0–65535).
- time time-out - Timeout in milliseconds to wait for each reply, from 50 to 65535 milliseconds. The default is 2000 milliseconds (50–65535).
- source source-address - Source address (Unicast IPv4 address or global Unicast IPv6 address).

Default Usage

N/A

Command Mode

Privileged EXEC mode

User Guidelines

Press Esc to stop pinging. Following are sample results of the ping command:

- Destination does not respond - If the host does not respond, a “no answer from host” appears within 10 seconds.
- Destination unreachable - The gateway for this destination indicates that the destination is unreachable.
- Network or host unreachable - The switch found no corresponding entry in the route table.

When using the ping ipv6 command to check network connectivity of a directly attached host using its link local address, the egress interface may be specified in the IPv6 format. If the egress interface is not specified, the default interface is selected.

When using the ping ipv6 command with a Multicast address, the information displayed is taken from all received echo responses.

When the source keyword is configured and the source address is not an address of the switch, the command is halted with an error message and pings are not sent.

Examples

Example 1 - Ping an IP address.

```
switchxxxxxx> ping ip 10.1.1.1
Pinging 10.1.1.1 with 64 bytes of data:
64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms
----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11
```

Example 2 - Ping a site.

```
switchxxxxxx> ping ip yahoo.com
Pinging yahoo.com [66.218.71.198] with 64 bytes of data:
64 bytes from 66.218.71.198: icmp_seq=0. time=11 ms
64 bytes from 66.218.71.198: icmp_seq=1. time=8 ms
64 bytes from 66.218.71.198: icmp_seq=2. time=8 ms
64 bytes from 66.218.71.198: icmp_seq=3. time=7 ms
----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss round-trip (ms)
min/avg/max = 7/8/11
```

Example 3 - Ping an IPv6 address.

```
switchxxxxxx> ping ipv6 3003::11
Pinging 3003::11 with 64 bytes of data:
64 bytes from 3003::11: icmp_seq=1. time=0 ms
64 bytes from 3003::11: icmp_seq=2. time=50 ms
64 bytes from 3003::11: icmp_seq=3. time=0 ms
64 bytes from 3003::11: icmp_seq=4. time=0 ms
----3003::11 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss round-trip (ms)
min/avg/max = 0/12/50
switchxxxxxx> ping ipv6 FF02::1
Pinging FF02::1 with 64 bytes of data:
64 bytes from FF02::1: icmp_seq=1. time=0 ms
64 bytes from FF02::1: icmp_seq=1. time=70 ms
64 bytes from FF02::1: icmp_seq=2. time=0 ms
64 bytes from FF02::1: icmp_seq=1. time=1050 ms
64 bytes from FF02::1: icmp_seq=2. time=70 ms
64 bytes from FF02::1: icmp_seq=2. time=1050 ms
64 bytes from FF02::1: icmp_seq=3. time=0 ms
64 bytes from FF02::1: icmp_seq=3. time=70 ms
64 bytes from FF02::1: icmp_seq=4. time=0 ms
64 bytes from FF02::1: icmp_seq=3. time=1050 ms
64 bytes from FF02::1: icmp_seq=4. time=70 ms
64 bytes from FF02::1: icmp_sq=4. time=1050 ms
---- FF02::1 PING Statistics----
4 packets transmitted, 12 packets received
```

24.2. telnet

The `telnet` EXEC mode command logs on to a host that supports Telnet.

Syntax

- telnet {ip-address | hostname} [port] [keyword...]

Parameters

- ip-address - Specifies the destination host IP address (IPv4 or IPv6).
- hostname - Hostname to ping (Length: 1-158 characters. Maximum label size for each part of the host name: 58.)
- port - Specifies the decimal TCP port number or one of the keywords listed in the Ports table in the User Guidelines.
- keyword - Specifies the one or more keywords listed in the Keywords table in the User Guidelines.

Default Configuration

The default port is the Telnet port (23) on the host.

Command Mode

Privileged EXEC mode

User Guidelines

Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To enter a Telnet sequence, press the escape sequence keys (Ctrl-shift-6) followed by a Telnet command character.

Special Telnet Sequences

Telnet Sequence	Purpose
Ctrl-shift-6-b	Break
Ctrl-shift-6-c	Interrupt Process (IP)
Ctrl-shift-6-h	Erase Character (EC)
Ctrl-shift-6-o	Abort Output (AO)
Ctrl-shift-6-t	Are You There? (AYT)
Ctrl-shift-6-u	Erase Line (EL)

At any time during an active Telnet session, available Telnet commands can be listed by pressing the `?/help` keys at the system prompt.

A sample of this list follows.

```
switchxxxxxx> ?/help
[Special telnet escape help]
^^ B sends telnet BREAK
^^ C sends telnet IP ^^ H sends telnet EC ^^ O sends telnet AO
^^ T sends telnet AYT
^^ U sends telnet EL
?/help suspends the session (return to system command prompt)
```

Several concurrent Telnet sessions can be opened, enabling switching between the sessions. To open a subsequent session, the current connection has to be suspended by pressing the escape sequence keys (Ctrl-shift-6) and x to return to the system command prompt. Then open a new connection with the telnet EXEC mode command.

This command lists concurrent Telnet connections to remote hosts that were opened by the current Telnet session to the local device. It does not list Telnet connections to remote hosts that were opened by other Telnet sessions.

Keywords Table

Options	Description
/echo	Enables local echo.
/quiet	Prevents onscreen display of all messages from the software.
/source-interface	Specifies the source interface.
/stream	Turns on stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols.
Ctrl-shift-6 x	Returns to the System Command Prompt.

Ports Table

Keyword	Description	Port Number
BGP	Border Gateway Protocol	179
chargen	Character generator	19
cmd	Remote commands	514
daytime	Daytime	13
discard	Discard	9
domain	Domain Name Service	53
echo	Echo	7
exec	Exec	512
finger	Finger	79
ftp	File Transfer Protocol	21
ftp-data	FTP data connections	20
gopher	Gopher	70
hostname	NIC hostname server	101
ident	Ident Protocol	113

irc	Internet Relay Chat	194
klogin	Kerberos login	543
kshell	Kerberos shell	544
login	Login	513
lpd	Printer service	515
nntp	Network News Transport Protocol	119
pim-auto-r p	PIM Auto-RP	496
pop2	Post Office Protocol v2	109
pop3	Post Office Protocol v3	110
smtp	Simple Mail Transport Protocol	25
sunrpc	Sun Remote Procedure Call	111
syslog	Syslog	514
tacacs	TAC Access Control System	49
talk	Talk	517
telnet	Telnet	23
time	Time	37
uucp	Unix-to-Unix Copy Program	540
whois	Nickname	43
www	World Wide Web	80

Example

The following example displays logging in to IP address 176.213.10.50 via Telnet.

```
switchxxxxxx> telnet 176.213.10.50
```

24.3. traceroute

To display the routes that packets will take when traveling to their destination, use the `traceroute` EXEC mode command.

Syntax

- traceroute ip {ipv4-address | hostname} [size packet_size] [ttl max-ttl] [count packet_count] [timeout time_out] [source ip-address]
- traceroute ipv6 {ipv6-address | hostname} [size packet_size] [ttl max-ttl] [count packet_count] [timeout time_out] [source ip-address]

Parameters

- ip - Use IPv4 to discover the route.
- ipv6 - Use IPv6 to discover the route.
- ipv4-address - IPv4 address of the destination host.
- ipv6-address - IPv6 address of the destination host.

- hostname - Hostname to ping (Length: 1-158 characters. Maximum label size for each part of the host name: 58.)
- size packet_size - Number of bytes in the packet not including the VLAN tag. The default is 64 bytes. (IPv4:64-1518, IPv6: 68-1518)
- ttl max-ttl - The largest TTL value that can be used. The default is 30. The traceroute command terminates when the destination is reached or when this value is reached. (Range: 1–255)
- count packet_count - The number of probes to be sent at each TTL level. The default count is 3. (Range: 1–10)
- timeout time_out - The number of seconds to wait for a response to a probe packet. The default is 3 seconds. (Range: 1–60)
- source ip-address - One of the interface addresses of the device to use as a source address for the probes. The device selects the optimal source address by default. (Range: Valid IP address)

Default Usage

N/A

Command Mode

Privileged EXEC mode

User Guidelines

The traceroute command works by taking advantage of the error messages generated by routers when a datagram exceeds its time-to-live (TTL) value.

The traceroute command starts by sending probe datagrams with a TTL value of one. This causes the first router to discard the probe datagram and send back an error message. The traceroute command sends several probes at each TTL level and displays the round-trip time for each.

The traceroute command sends out one probe at a time. Each outgoing packet can result in one or two error messages. A "time exceeded” error message indicates that an intermediate router has seen and discarded the probe. A "destination unreachable" error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, the traceroute command prints an asterisk (*).

The traceroute command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with Esc.

The traceroute ipv6 command is not relevant to IPv6 link local addresses.

Example

```
switchxxxxxx> traceroute ip umaxp1.physics.lsa.umich.edu
Type Esc to abort.
Tracing the route to umaxp1.physics.lsa.umich.edu (141.211.101.64)
i2-gateway.stanford.edu (192.68.191.83) 0 msec 0 msec 0 msec
STAN.POS.calren2.NET (171.64.1.213) 0 msec 0 msec 0 msec
SUNV--STAN.POS.calren2.net (198.32.249.73) 1 msec 1 msec 1 msec
Abilene--QSV.POS.calren2.net (198.32.249.162) 1 msec 1 msec 1 msec
kscyng-snvang.abilene.ucaid.edu (198.32.8.103) 33 msec 35 msec 35 msec
iplsng-kscyng.abilene.ucaid.edu (198.32.8.80) 47 msec 45 msec 45 msec
so-0-2-0x1.aa1.mich.net (192.122.183.9) 56 msec 53 msec 54 msec
atm1-0x24.michnet8.mich.net (198.108.23.82) 56 msec 56 msec 57 msec
* * *
```

```
A-ARB3-LSA-NG.c-SEB.umnet.umich.edu(141.211.5.22)58 msec 58msec 58 msec
umaxp1.physics.lsa.umich.edu (141.211.101.64) 62 msec 63 msec 63 msec
Trace completed
```

The following table describes the significant fields shown in the display:

Field	Description
1	Indicates the sequence number of the router in the path to the host.
i2-gateway.stanford. edu	Host name of this router.
192.68.191.83	IP address of this router.
1 msec 1 msec 1 msec	Round-trip time for each of the probes that are sent.

The following are characters that can appear in the traceroute command output:

Field	Description
*	The probe timed out.
?	Unknown packet type.
A	Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.
F	Fragmentation required and DF is set.
H	Host unreachable.
N	Network unreachable.
P	Protocol unreachable.
Q	Source quench.
R	Fragment reassembly time exceeded
S	Source route failed.
U	Port unreachable.

25. IPv6 Commands

25.1. clear ipv6 neighbors

Use the `clear ipv6 neighbors` command in privileged EXEC mode to delete all entries in the IPv6 neighbor discovery cache, except static entries.

Syntax

- clear ipv6 neighbors

Parameters

N/A

Command Mode

Privileged EXEC mode

User Guidelines

Example

The following example deletes all entries, except static entries, in the neighbor discovery cache:

```
switchxxxxxx# clear ipv6 neighbors
```

25.2. ipv6 address

Use the `ipv6 address` command in Interface Configuration mode to configure a global unicast IPv6 address based on an IPv6 general prefix and enable IPv6 processing on an interface. To remove the address from the interface, use the no form of this command.

Syntax

- ipv6 address ipv6-address/prefix-length
- no ipv6 address [ipv6-address/prefix-length]

Parameters

- ipv6-address - Specifies the global unicast IPv6 address assigned to the interface. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- prefix-length - The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Default Configuration

No IP address is defined for the interface.

Command Mode

Interface Configuration mode

User Guidelines

The ipv6 address command cannot be applied to define an IPv6 address on an ISATAP interface.

Using the no IPv6 address command without arguments removes all manually-configured IPv6 addresses from an interface, including link local manually configured addresses.

Example

The following example defines the IPv6 global address 2001:DB8:2222:7272::72 on vlan 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 address 2001:DB8:2222:7272::72/64
switchxxxxxx(config-if)# exit
```

25.3. ipv6 address autoconfig

Use the `ipv6 address autoconfig` command in Interface Configuration mode to enable automatic configuration of IPv6 addresses using stateless auto configuration on an interface and enable IPv6 processing on the interface.

Addresses are configured depending on the prefixes received in Router Advertisement messages. To disable automatic configuration of IPv6 addresses and to remove the automatically configured address from the interface, use the no form of this command.

Syntax

- ipv6 address autoconfig
- no ipv6 address autoconfig

Parameters

N/A.

Default Configuration

Stateless Auto configuration is enabled.

Command Mode

Interface Configuration mode

User Guidelines

This command enables IPv6 on an interface (if it was disabled) and causes the switch to perform IPv6 stateless address auto-configuration to discover prefixes on the link and then to add the eui-64 based addresses to the interface.

Stateless auto configuration is applied only when IPv6 Forwarding is disabled.

When IPv6 forwarding is changed from disabled to enabled, and stateless auto configuration is enabled the switch stops stateless auto configuration and removes all stateless auto configured ipv6 addresses from all interfaces.

When IPv6 forwarding is changed from enabled to disabled and stateless auto configuration is enabled the switch resumes stateless auto configuration.

Additionally the ipv6 address autoconfig command enables on the interface the DHCPv6 Stateless client to receive DHCP stateless information and this information is received from a DHCPv6 server regardless whether IPv6 Forwarding is enabled or not.

Using the no form of the `ipv6 address` command without arguments removes all manually-configured IPv6 addresses from an interface, including link local manually-configured addresses.

Example

The following example assigns the IPv6 address automatically:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 address autoconfig
switchxxxxxx(config-if)# exit
```

25.4. ipv6 address eui-64

Use the `ipv6 address eui-64` command in Interface Configuration mode to configure a global unicast IPv6 address for an interface and enables IPv6 processing on the interface using an EUI-64 interface ID in the low order 64 bits of the address. To remove the address from the interface, use the no form of this command.

Syntax

- ipv6 address ipv6-prefix/prefix-length eui-64
- no ipv6 address [ipv6-prefix/prefix-length eui-64]

Parameters

- ipv6-prefix - Specifies the global unicast IPv6 address assigned to the interface. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- prefix-length - The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Default Configuration

No IP address is defined for the interface.

Command Mode

Interface Configuration mode

User Guidelines

If the value specified for the prefix-length argument is greater than 64 bits, the prefix bits have precedence over the interface ID.

The IPv6 address is built from ipv6-prefix and the EUI-64 Interface ID by the following way:

- The first prefix-length bits are taken from ipv6-prefix.
- If prefix-length < 64 then
- The following (64-prefix-length) bits are filled by 0s.
- The last 64 bits are taken from the EUI-64 Interface ID.
- If prefix-length equals to 64 then the following 64 bits are taken from the EUI-64 Interface ID.
- If prefix-length > 64 then the following (128-prefix-length) bits are taken from the last (64-(prefix-length -64)) bits of the EUI-64 Interface ID.

If the switch detects another host using one of its IPv6 addresses, it adds the IPv6 address and displays an error message on the console.

Using the no form of the `ipv6 address` command without arguments removes all manually-configured IPv6 addresses from an interface, including link local manually-configured addresses.

Example

The following example enables IPv6 processing on VLAN 1, configures IPv6 global address 2001:0DB8:0:1::/64 and specifies an EUI-64 interface ID in the low order 64 bits of the address:

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 address 2001:0DB8:0:1::/64 eui-64
switchxxxxxx(config-if)# exit
```

25.5. ipv6 address link-local

Use the `ipv6 address link-local` command in Interface Configuration mode to configure an IPv6 link local address for an interface and enable IPv6 processing on the interface. To remove the manually configured link local address from the interface, use the no form of this command.

Syntax

- ipv6 address ipv6-prefix link-local
- no ipv6 address [link-local]

Parameters

- ipv6-address - Specifies the IPv6 network assigned to the interface. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.

Default Configuration

The default Link-local address is defined.

Command Mode

Interface Configuration mode

User Guidelines

The switch automatically generates a link local address for an interface when IPv6 processing is enabled on the interface, typically when an IPv6 address is configured on the interface. To manually specify a link local address to be used by an interface, use the `ipv6 address link-local` command.

The ipv6 address link-local command cannot be applied to define an IPv6 address on an ISATAP interface.

Using the no form of the `ipv6 address` command without arguments removes all manually-configured IPv6 addresses from an interface, including link local manually-configured addresses.

Example

The following example enables IPv6 processing on VLAN 1 and configures FE80::260:3EFF:FE11:6770 as the link local address for VLAN 1:

interface vlan 1

```
switchxxxxxx(config-if)# ipv6 address FE80::260:3EFF:FE11:6770 link-local
switchxxxxxx(config-if)# exit
```

25.6. ipv6 default-gateway

Use the `ipv6 default-gateway` Global Configuration mode command to define an IPv6 default gateway. To remove the IPv6 default gateway, use the no form of this command.

Syntax

- ipv6 default-gateway ipv6-address

- no ipv6 default-gateway [ipv6-address]

Parameters

- ipv6-address - Specifies the IPv6 address of an IPv6 router that can be used to reach a network.

Default Configuration

No default gateway is defined.

Command Mode

Global Configuration mode

User Guidelines

The command is an alias of the `ipv6 route` command with the predefined (default) route:

```
ipv6 route ::/0 ipv6-address | interface-id
```

See the definition of the `ipv6 route` command for details.

Examples

Example 1. The following example defines a default gateway with a global IPv6 address:

```
ipv6 default-gateway 5::5
```

Example 2. The following example defines a default gateway with a link-local IPv6 address:

```
switchxxxxxx(config)# ipv6 default-gateway FE80::260:3EFF:FE11:6770%vlan1
```

25.7. ipv6 enable

Use the `ipv6 enable` command in Interface Configuration mode to enable IPv6 processing on an interface.

To disable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the no form of this command.

Syntax

- ipv6 enable
- no ipv6 enable

Parameters

N/A.

Default Configuration

IPv6 interface is disabled.

Command Mode

Interface Configuration mode

User Guidelines

This command automatically configures an IPv6 link-local Unicast address on the interface while also enabling the interface for IPv6 processing. The no ipv6 enable command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

Example

The following example enables VLAN 1 for the IPv6 addressing mode.

interface vlan 1

```
switchxxxxxx(config-if)# ipv6 enable
switchxxxxxx(config-if)# exit
```

25.8. ipv6 icmp error-interval

Use the `ipv6 icmp error-interval` command in Global Configuration mode to configure the interval and bucket size for IPv6 ICMP error messages. To return the interval to its default setting, use the no form of this command.

Syntax

- ipv6 icmp error-interval milliseconds [bucketsize]
- no ipv6 icmp error-interval

Parameters

- milliseconds - Time interval between tokens being placed in the bucket. Each token represents a single ICMP error message. The acceptable range is from 0 to 2147483647. A value of 0 disables ICMP rate limiting.
- bucketsize - Maximum number of tokens stored in the bucket. The acceptable range is from 1 to 200.

Default Configuration

The default interval is 100ms and the default bucketsize is 10 i.e. 100 ICMP error messages per second.

Command Mode

Global Configuration mode

User Guidelines

Use this command to limit the rate at which IPv6 ICMP error messages are sent. A token bucket algorithm is used with one token representing one IPv6 ICMP error message. Tokens are placed in the virtual bucket at a specified interval until the maximum number of tokens allowed in the bucket is reached.

The milliseconds argument specifies the time interval between tokens arriving in the bucket. The optional bucketsize argument is used to define the maximum number of tokens allowed in the bucket. Tokens are removed from the bucket

when IPv6 ICMP error messages are sent, which means that if the bucketsize is set to 20, a rapid succession of 20 IPv6 ICMP error messages can be sent. When the bucket is empty of tokens, IPv6 ICMP error messages are not sent until a new token is placed in the bucket.

Average Packets Per Second = (1000/ milliseconds) * bucketsize.

To disable ICMP rate limiting, set the milliseconds argument to zero.

Example

The following example shows an interval of 50 milliseconds and a bucket size of 20 tokens being configured for IPv6 ICMP error messages:

```
switchxxxxxx(config)# ipv6 icmp error-interval 50 20
```

25.9. ipv6 link-local default zone

Use the `ipv6 link-local default zone` command to configure an interface to egress a link local packet without a specified interface or with the default zone 0.

Use the no form of this command to return the default link local interface to the default value.

Syntax

- Ipv6 link-local default zone interface-id
- no Ipv6 link-local default zone

Parameters

- interface-id - Specifies the interface that is used as the egress interface for packets sent without a specified IPv6 interface identifier or with the default 0 identifier.

Default

By default, link local default zone is disabled.

Command Mode

Global Configuration mode

Example

The following example defines VLAN 1 as a default zone:

```
switchxxxxxx(config)# ipv6 link-local default zone vlan1
```

25.10. ipv6 nd dad attempts

Use the `ipv6 nd dad attempts` command in Interface Configuration mode to configure the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection is performed on the Unicast IPv6 addresses of the interface.

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

Syntax

- ipv6 nd dad attempts value
- no ipv6 nd dad attempts

Parameters

- value - The number of neighbor solicitation messages. The acceptable range is from 0 to 600. Configuring a value of 0 disables duplicate address detection processing on the specified interface; a value of 1 configures a single transmission without follow-up transmissions.

Default Configuration

1

Command Mode

Interface Configuration mode

User Guidelines

Duplicate address detection verifies the uniqueness of new Unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while

duplicate address detection is performed). Duplicate address detection uses neighbor solicitation messages to verify the uniqueness of Unicast IPv6 addresses.

The DupAddrDetectTransmits node configuration variable (as specified in RFC 4862, IPv6 Stateless Address Autoconfiguration) is used to automatically determine the number of consecutive neighbor solicitation messages that are sent on an interface, while duplicate address detection is performed on a tentative Unicast IPv6 address.

The interval between duplicate address detection, neighbor solicitation messages (the duplicate address detection timeout interval) is specified by the neighbor discovery-related variable RetransTimer (as specified in RFC 4861, Neighbor Discovery for IPv6), which is used to determine the time between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor. This is the same management variable used to specify the interval for neighbor solicitation messages during address resolution and neighbor unreachability detection. Use the `ipv6 nd ns-interval` command to configure the interval between neighbor solicitation messages that are sent during duplicate address detection.

Duplicate address detection is suspended on interfaces that are administratively down. While an interface is administratively down, the Unicast IPv6 addresses assigned to the interface are set to a pending state. Duplicate address detection is automatically restarted on an interface when the interface returns to being administratively up.

An interface returning to administratively up, restarts duplicate address detection for all of the Unicast IPv6 addresses on the interface. While duplicate address detection is performed on the link-local address of an interface, the state for the other IPv6 addresses is still set to TENTATIVE. When duplicate address detection is completed on the link-local address, duplicate address detection is performed on the remaining IPv6 addresses.

When duplicate address detection identifies a duplicate address, the state of the address is set to DUPLICATE and the address is not used. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface and an error SYSLOG message is issued.

If the duplicate address is a global address of the interface, the address is not used and an error SYSLOG message is issued.

All configuration commands associated with the duplicate address remain as configured while the state of the address is set to DUPLICATE.

If the link-local address for an interface changes, duplicate address detection is performed on the new link-local address and all of the other IPv6 address associated with the interface are regenerated (duplicate address detection is performed only on the new link-local address).

Example

The following example configures five consecutive neighbor solicitation messages to be sent on VLAN 1 while duplicate address detection is being performed on the tentative Unicast IPv6 address of the interface. The example also disables duplicate address detection processing on VLAN 2.

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 nd dad attempts 5
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# ipv6 nd dad attempts 0
switchxxxxxx(config-if)# exit
```

25.11. ipv6 neighbor

Use the `ipv6 neighbor` command in Global Configuration mode to configure a static entry in the IPv6 neighbor discovery cache. To remove a static IPv6 entry from the IPv6 neighbor discovery cache, use the no form of this command.

Syntax

- ipv6 neighbor ipv6-address interface-id mac-address
- no ipv6 neighbor [[ipv6-address] interface-id]

Parameters

- ipv6-address - Specified IPv6 address. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- interface-id - Specified interface identifier.
- mac-address - Interface MAC address.

Default Configuration

Static entries are not configured in the IPv6 neighbor discovery cache.

Command Mode

Global Configuration mode

User Guidelines

This command is similar to the `arp` command.

Use the `ipv6 neighbor` command to add a static entry in the IPv6 neighbor discovery cache.

If the specified IPv6 address is a global IPv6 address it must belong to one of static on-link prefixes defined in the interface. When a static on-link prefix is deleted all static entries in the IPv6 neighbor discovery cache corresponding the prefix is deleted to.

If an entry for the specified IPv6 address already exists in the neighbor discovery cache, learned through the IPv6 neighbor discovery process, the entry is automatically converted to a static entry.

Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.

Use the no ipv6 neighbor ipv6-address interface-id command to remove the one given static entry on the given interface. The command does not remove the entry from the cache, if it is a dynamic entry, learned from the IPv6 neighbor discovery process.

Use the `no ipv6 neighbor interface-id` command to delete the all static entries on the given interface.

Use the `no ipv6 neighbor` command to remove the all static entries on all interfaces.

Use the `show ipv6 neighbors` command to view static entries in the IPv6 neighbor discovery cache. A static entry in the IPv6 neighbor discovery cache can have one of the following states:

- NCMP (Incomplete) - The interface for this entry is down.
- REACH (Reachable) - The interface for this entry is up.

Note:
Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the INCMP and REACH states are different for dynamic and static cache entries.

Examples

Example 1. The following example configures a static entry in the IPv6 neighbor discovery cache for a neighbor with the IPv6 address 2001:0DB8::45A and link-layer address 0002.7D1A.9472 on VLAN 1:

```
switchxxxxxx(config)# ipv6 neighbor 2001:0DB8::45A vlan1 0002.7D1A.9472
```

Example 2. The following example deletes the static entry in the IPv6 neighbor discovery cache for a neighbor with the IPv6 address 2001:0DB8::45A and link-layer address 0002.7D1A.9472 on VLAN 1:

```
switchxxxxxx(config)# no ipv6 neighbor 2001:0DB8::45A vlan1
```

Example 3. The following example deletes all static entries in the IPv6 neighbor discovery cache on VLAN 1:

```
switchxxxxxx(config)# no ipv6 neighbor vlan1
```

Example 4. The following example deletes all static entries in the IPv6 neighbor discovery cache on all interfaces:

```
switchxxxxxx(config)# no ipv6 neighbor
```

25.12. ipv6 route

Use the `ipv6 route` command in Global Configuration mode to establish static IPv6 routes. To remove a previously configured static route, use the no form of this command.

Syntax

- ipv6 route ipv6-prefix/prefix-length {next--ipv6-address | interface-id} [metric]
- no ipv6 route ipv6-prefix/prefix-length {next--ipv6-address | interface-id}

Parameters

- ipv6-prefix - IPv6 network that is the destination of the static route. Can also be a host name when static host routes are configured.
- /prefix-length - Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
- next-ipv6-address - IPv6 address of the next hop that can be used to reach the specified network.
  - If the next--ipv6-address argument is a link local address it must be defined in the zone format: IPv6 Zone Format> ::= IPv6-Link-Local-Address%Interface-ID
  - The interface-id argument must be coded without spaces.
- interface-id - Outgoing Interface identifier. This argument can be applied only to point-to-point interfaces (manual IPv6 over IPv4 tunnels).
- Metric - Static route metric. Acceptable values are from 1 to 65535. The default value is 1.

Default Configuration

Static entries are not configured in the IPv6 neighbor discovery cache.

Command Mode

Global Configuration mode

User Guidelines

If the next IPv6 address is a global IPv6 address, it should belong to a static on-link prefix. When an on-link prefix is removed or is changed to non on-link prefix, the static routes with next hop belonging to the prefix are removed from the configuration.

Examples

Example 1: The following example defines a static route with a global next hop:

```
switchxxxxxx(config)# ipv6 route 2001::/64 5::5 10
```

Example 2: The following example defines a static route with a link-local next hop:

```
switchxxxxxx(config)# ipv6 route 2001:DB8:2222::/48
FE80::260:3EFF:FE11:6770%vlan1 12
```

Example 3: The following example defines a static route on manual tunnel 1:

```
switchxxxxxx(config)# ipv6 route 2001:DB8:2222::/48 tunnel1
```

25.13. ipv6 unicast-routing

Use the `ipv6 unicast-routing` command in Global Configuration mode to enable the forwarding of IPv6 Unicast datagrams. To disable the forwarding of IPv6 Unicast datagrams, use the no form of this command.

Syntax

- ipv6 unicast-routing
- no ipv6 unicast-routing

Parameters

N/A.

Default Configuration

IPv6 Unicast routing is disabled.

Command Mode

Global Configuration mode

Example

The following example enables the forwarding of IPv6 Unicast datagrams:

```
switchxxxxxx(config)# ipv6 unicast-routing
```

25.14. ipv6 unreachables

Use the `ipv6 unreachables` command in Interface Configuration mode to enable the generation of Internet Control Message Protocol for IPv6 (ICMPv6) unreachable messages for any packets arriving on a specified interface.

To prevent the generation of unreachable messages, use the no form of this command.

Syntax

- ipv6 unreachables
- no ipv6 unreachables

Parameters

N/A.

Default Configuration

The sending of ICMP IPv6 unreachable messages is enabled.

Command Mode

Interface Configuration mode

User Guidelines

If the switch receives a Unicast packet destined for itself that uses a protocol it does not recognize, it sends an ICMPv6 unreachable message to the source.

If the switch receives a datagram that it cannot deliver to its ultimate destination because it knows of no route to the destination address, it replies to the originator of that datagram with an ICMP host unreachable message.

Example

The following example disables the generation of ICMPv6 unreachable messages, as appropriate, on an interface:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# no ipv6 unreachables
switchxxxxxx(config-if)# exit
```

25.15. show ipv6 interface

Use the `show ipv6 interface` command in user EXEC or privileged EXEC mode to display the usability status of interfaces configured for IPv6.

Syntax

- show ipv6 interface [brief] | [interface-id]

Parameters

- brief - Displays a brief summary of IPv6 status and configuration for each interface where IPv6 is defined.
- interface-id - Interface identifier about which to display information.

Default Configuration

Option brief - all IPv6 interfaces are displayed.

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

Use this command to validate the IPv6 status of an interface and its configured addresses. This command also displays the parameters that IPv6 uses for operation on this interface and any configured features.

If the interface’s hardware is usable, the interface is marked up.

If you specify an optional interface identifier, the command displays information only about that specific interface. For a specific interface, you can enter the prefix keyword to see the IPv6 neighbor discovery (ND) prefixes that are configured on the interface.

Examples

Example 1. The show ipv6 interface command displays information about the specified interface:

```
switchxxxxxx# show ipv6 interface vlan 1
VLAN 1 is up/up
IPv6 is enabled, link-local address is FE80::0DB8:12AB:FA01
Global unicast address(es):
Ipv6 Global Address Type
2000:0DB8::2/64 (ANY) Manual
2000:0DB8::2/64 Manual 2000:1DB8::2011/64 Manual Joined group address(es):
FF02::1
FF02::2
FF02::1:FF11:6770
MTU is 1500 bytes
ICMP error messages limited interval is 100ms; Bucket size is 10 tokens
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds Stateless autoconfiguration is enabled.
MLD Version is 2
Field Descriptions:
vlan 1 is up/up - Indicates the interface status: administrative/operational.
IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample
output) - Indicates that IPv6 is enabled, stalled, or disabled on the interface.
If IPv6 is enabled, the interface is marked Enabled. If duplicate address
detection processing identified the link-local address of the interface as being
a duplicate address, the processing of IPv6 packets is disabled on the interface
and the interface is marked Stalled. If IPv6 is not enabled, the interface is
marked Disabled.
link-local address - Displays the link-local address assigned to the interface.
Global unicast address(es): - Displays the global Unicast addresses assigned to
the interface. The type is manual or autoconfig.
Joined group address(es): - Indicates the Multicast groups to which this
interface belongs.
MTU is 1500 bytes - Maximum transmission unit of the interface.
ICMP error messages - Specifies the minimum interval (in milliseconds) between
error messages sent on this interface.
ND DAD - The state of duplicate address detection on the interface (enabled or
disabled).
number of DAD attempts: - Number of consecutive neighbor solicitation messages
that are sent on the interface while duplicate address detection is performed.
ND reachable time - Displays the neighbor discovery reachable time (in
milliseconds) assigned to this interface.
MLD Version - Version of MLD
```

Example 2. The following command with the brief keyword displays information about all interfaces that IPv6 is defined on:

```
switchxxxxxx# show ipv6 interface brief
Interface Interface IPv6 Link Local MLD Number of
 State State IPv6 Address Version Global Addresses --------- --------- ------- -
---------------- ------- ----------------
vlan 1 up/up enabled FE80::0DB8:12AB:FA01 1 1 vlan 2 up/up stalled
FE80::0DB8:12AB:FA01 1 1 vlan 3 up/down enabled FE80::0DB8:12AB:FA01 1 3 vlan 4
down/down enabled FE80::0DB8:12AB:FA01 2 2 vlan 5 up/up enabled
FE80::0DB8:12AB:FA01 1 1 vlan 100 up/up enabled FE80::0DB8:12AB:FA01 1 1 vlan
1000 up/up stalled FE80::0DB8:12AB:FA01 1 1
```

25.16. show ipv6 link-local default zone

Use the `show ipv6 link-local default zone` command in user EXEC or privileged EXEC mode to display the IPv6 link local default zone.

Syntax

- show ipv6 link-local default zone

Command Mode

User EXEC mode

Privileged EXEC mode

Examples

Example 1. The following example displays the default zone when it is defined:

```
switchxxxxxx# show ipv6 link-local default zone
Link Local Default Zone is VLAN 1
```

Example 2. The following example displays the default zone when it is not defined:

```
switchxxxxxx# show ipv6 link-local default zone
Link Local Default Zone is not defined
```

25.17. show ipv6 neighbors

Use the `show ipv6 neighbors` command in User EXEC or Privileged EXEC mode to display IPv6 neighbor discovery (ND) cache information.

Syntax

- show ipv6 neighbors [interface-id | ipv6-address | ipv6-hostname]

Parameters

- interface-id - Specifies the identifier of the interface from which IPv6 neighbor information is to be displayed.
- ipv6-address - Specifies the IPv6 address of the neighbor. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- ipv6-hostname - Specifies the IPv6 host name of the remote networking device.

Default Configuration

All IPv6 ND cache entries are listed.

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

When the interface-id argument is not specified, cache information for all IPv6 neighbors is displayed. Specifying the interface-id argument displays only cache information about the specified interface.

Examples

Example 1. The following is sample output from the show ipv6 neighbors command when entered with an interface-id:

```
switchxxxxxx# show ipv6 neighbors vlan 1
IPv6 Address Age Link-layer Addr State Interface Router
2000:0:0:4::2 0 0003.a0d6.141e REACH VLAN1 Yes
3001:1::45a - 0002.7d1a.9472 REACH VLAN1 -
FE80::203:A0FF:FED6:141E 0 0003.a0d6.141e REACH VLAN1 No
```

Example 2. The following is sample output from the show ipv6 neighbors command when entered with an IPv6 address:

```
switchxxxxxx# show ipv6 neighbors 2000:0:0:4::2
IPv6 Address Age Link-layer Addr State Interface Router
2000:0:0:4::2 0 0003.a0d6.141e REACH VLAN1 Yes
Field Descriptions:
Total number of entries - Number of entries (peers) in the cache.
IPv6 Address - IPv6 address of neighbor or interface.
Age - Time (in minutes) since the address was confirmed to be reachable. A
hyphen (-) indicates a static entry.
Link-layer Addr - MAC address. If the address is unknown, a hyphen (-) is
displayed.
Interface - Interface which the neighbor is connected to.
Router - Specifies if the neighbor is a Router. A hyphen (-) is displayed for
static entries.
```

25.18. show ipv6 route

Use the `show ipv6 route` command in user EXEC or privileged EXEC mode to display the current contents of the IPv6 routing table.

Syntax

- show ipv6 route [ipv6-address | ipv6-prefix/prefix-length | protocol | interface interface-id]

Parameters

- ipv6-address - Displays routing information for a specific IPv6 address. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- ipv6-prefix - Displays routing information for a specific IPv6 network. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.

- /prefix-length - The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
- protocol - Displays routes for the specified routing protocol using any of these keywords: bgp, isis, ospf, or rip; or displays routes for the specified type of route using any of these keywords: connected, static, nd, or icmp.
- interface interface-id - Identifier of an interface.

Default Configuration

All IPv6 routing information for all active routing tables is displayed.

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

This command provides output similar to the show ip route command, except that the information is IPv6-specific.

When the ipv6-address or ipv6-prefix/prefix-length argument is specified, a longest match lookup is performed from the routing table and only route information for that address or network is displayed. When the icmp, nd, connected, local, or static keywords are specified, only that type of route is displayed. When the interface-id argument are specified, only the specified interface-specific routes are displayed.

Example

The following is sample output from the show ipv6 route command when the command is entered without an IPv6 address or prefix specified:

```
switchxxxxxx# show ipv6 route
Codes: > - Best
 S - Static, C - Connected(from ipv6 address), I - ICMP Redirect, ND -
Router Advertisment
[d/m]: d - route’s distance, m - route’s metric
IPv6 Routing Table - 4 entries S> ::/0 [1/1] via:: fe80::77 VLAN 1 ND> ::/0
[3/2] via:: fe80::200:cff:fe4a:dfa8 VLAN 1 Lifetime 1784 sec C> 3002:1:1:1:1/64
[0/0] via:: VLAN 1 ND> 3004:1:1:1:1/64 [0/0] via:: VLAN 100 Lifetime 1784 sec
```

25.19. show ipv6 route summary

Use the `show ipv6 route summary` command in User EXEC or Privileged EXEC mode to display the current contents of the IPv6 routing table in summary format.

Syntax

- show ipv6 route summary

Parameters

N/A.

Command Mode

User EXEC mode

Privileged EXEC mode

Example

The following is sample output from the show ipv6 route summary command:

```
switchxxxxxx# show ipv6 route summary
IPv6 Routing Table Summary - 97 entries
37 local, 35 connected, 25 static
Number of prefixes:
/16: 1, /28: 10, /32: 5, /35: 25, /40: 1, /64: 9
/96: 5, /112: 1, /127: 4, /128: 36
```

25.20. show ipv6 static

Use the `show ipv6 static` command in user EXEC or privileged EXEC mode to display the current static routes of the IPv6 routing table.

Syntax

- show ipv6 static [ipv6-address | ipv6-prefix/prefix-length] [interface interface-id][detail]

Parameters

- ipv6-address - Provides routing information for a specific IPv6 address. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- ipv6-prefix - Provides routing information for a specific IPv6 network. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- /prefix-length - Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
- interface interface-id - Identifier of an interface.
- detail - Specifies for invalid routes, the reason why the route is not valid.

Default Configuration

All IPv6 static routing information for all active routing tables is displayed.

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

When the ipv6-address or ipv6-prefix/prefix-length argument is specified, a longest match lookup is performed from the routing table and only route information for that address or network is displayed. Only the information matching the criteria specified in the command syntax is displayed. For example, when the interface-id argument is specified, only the specified interface-specific routes are displayed.

When the detail keyword is specified, the reason why the route is not valid is displayed for invalid direct or fully specified routes.

Examples

Example 1: The following is sample output from the `show ipv6 static` command without specified options:

```
switchxxxxxx# show ipv6 static
IPv6 Static routes Code: * - installed in Routing Information Base (RIB)
IPv6 Static routes distance is 1
* 3000::/16, interface VLAN1, metric 1
* 4000::/16, via nexthop 2001:1::1, metric 1
  5000::/16, interface VLAN2, metric 1
* 5555::/16, via nexthop 4000::1, metric 1
  5555::/16, via nexthop 9999::1, metric 1
* 5555::/16, via nexthop 4001:AF00::1, metric 1
* 6000::/16, via nexthop 2007::1, metric 1
```

Example 2: The following is sample output from the `show ipv6 route` command when entered with the IPv6 prefix 2001:200::/35:

```
switchxxxxxx# show ipv6 static 2001:200::/35
IPv6 Static routes Code: * - installed in Routing Information Base (RIB)
IPv6 Static routes distance is 1
* 2001:200::/35, via nexthop 4000::1, metric 1
  2001:200::/35, via nexthop 9999::1, metric 1
* 2001:200::/35, interface VLAN1, metric 1
```

Example 3: The following is sample output from the show ipv6 route command when entered with the interface VLAN 1:

```
switchxxxxxx# show ipv6 static interface vlan 1
IPv6 Static routes Code: * - installed in Routing Information Base (RIB)
IPv6 Static routes distance is 1
* 5000::/16, interface VLAN1, metric 1
```

Example 4: The following is sample output from the show ipv6 route command with the detail keyword:

```
switchxxxxxx# show ipv6 static detail
IPv6 Static routes Code: * - installed in Routing Information Base (RIB)
IPv6 Static routes distance is 1
* 3000::/16, interface VLAN1, metric 1
* 4000::/16, via nexthop 2001:1::1, metric 1
  5000::/16, interface VLAN2, metric 1
Interface is down
* 5555::/16, via nexthop 4000::1, metric 1
  5555::/16, via nexthop 9999::1, metric 1
Route does not fully resolve
* 5555::/16, via nexthop 4001:AF00::1, metric 1
* 6000::/16, via nexthop 2007::1, metric 1
```

26. IPv6 Prefix List Commands

26.1. clear ipv6 prefix-list

Use the `clear ipv6 prefix-list` command in privileged EXEC mode to reset the hit count of the IPv6 prefix list entries.

Syntax

- clear ipv6 prefix-list [prefix-list-name [ipv6-prefix/prefix-length]]

Parameters

- prefix-list-name - The name of the prefix list from which the hit count is to be cleared.
- ipv6-prefix - The IPv6 network from which the hit count is to be cleared. This argument must be in the form documented in RFC 4293 where the address is specified in hexadecimal using 16-bit values between colons.
- /prefix-length - The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Default Configuration

The hit count is automatically cleared for all IPv6 prefix lists.

Command Mode

Privileged EXEC mode

User Guidelines

The hit count is a value indicating the number of matches to a specific prefix list entry.

Example

The following example clears the hit count from the prefix list entries for the prefix list named first_list that match the network mask 2001:0DB8::/35:

```
switchxxxxxx# clear ipv6 prefix-list first_list 2001:0DB8::/35
```

26.2. ipv6 prefix-list

Use the `ipv6 prefix-list` command in Global Configuration mode to create an entry in an IPv6 prefix list. To delete the entry, use the no form of this command.

Syntax

- ipv6 prefix-list list-name [seq number] {{deny|permit} ipv6-prefix/prefix-length [ge ge-length] [le le-length]} | description text
- no ipv6 prefix-list list-name [seq number]

Parameters

- list-name - Name of the prefix list. The name may contain up to 32 characters.
- seq seq-number - Sequence number of the prefix list entry being configured. This is an integer value from 1 to 4294967294.
- deny - Denies networks that matches the condition.
- permit - Permits networks that matches the condition.
- ipv6-prefix - IPv6 network assigned to the specified prefix list. This argument must be in the form documented in RFC 4293 where the address is specified in hexadecimal - using 16-bit values between colons.

- /prefix-length - Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value from 0 to 128. The zero prefix-length may be used only with the zero ipv6-prefix (::).
- description text - Text that can be up to 80 characters in length.
- ge ge-value - Specifies a prefix length greater than or equal to the /prefix-length argument. It is the lowest value of a range of the length (the “from” portion of the length range).
- le le-value - Specifies a prefix length greater than or equal to the /prefix-length argument. It is the highest value of a range of the length (the “to” portion of the length range).

Default Configuration

No prefix list is created.

Command Mode

Global Configuration mode

User Guidelines

This command without the seq keyword adds the new entry after the last entry of the prefix list with the sequence number equals to the last number plus 5. For example, if the last configured sequence number is 43, the new entry will have the sequence number of 48. If the list is empty, the first prefix-list entry is assigned the number 5 and subsequent prefix list entries increment by 5.

This command with the seq keyword puts the new entry into the place specified by the parameter, if an entry with the number exists it is replaced by the new one.

This command without the seq keyword removes the prefix list.

The no version of this command with the seq keyword removes the specified entry.

The sequence number of a prefix list entry determines the order of the entries in the list. The router compares network addresses to the prefix list entries. The router begins the comparison at the top of the prefix list, with the entry having the lowest sequence number.

If multiple entries of a prefix list match a prefix, the entry with the lowest sequence number is considered the real match. Once a match or deny occurs, the router does not go through the rest of the prefix list. For efficiency, you might want to put the most common permits or denies near the top of the list, using the seq-number argument.

The `show ipv6 prefix-list` command displays the sequence numbers of entries.

IPv6 prefix lists are used to specify certain prefixes or a range of prefixes that must be matched before a permit or deny statement can be applied. Two operand keywords can be used to designate a range of prefix lengths to be matched. A prefix length of less than, or equal to, a value is configured with the le keyword. A prefix length greater than, or equal to, a value is specified using the ge keyword. The ge and le keywords can be used to specify the range of the prefix length to be matched in more detail than the usual ipv6-prefix/prefix-length argument.

- For a candidate prefix to match against a prefix list entry the following conditions must exist: The candidate prefix must match the specified prefix list and prefix length entry
- The value of the optional le keyword specifies the range of allowed prefix lengths from 0 up to the value of the le-length argument, and including, this value.

- The value of the optional ge keyword specifies the range of allowed prefix lengths from the value of the ge-length argument up to, and including, 128. Note that the first condition must match before the other conditions take effect.

An exact match is assumed when the ge or le keywords are not specified. If only one keyword operand is specified then the condition for that keyword is applied, and the other condition is not applied. The prefix-length value must be less than the ge value. The ge value must be less than, or equal to, the le value. The le value must be less than or equal to 128.

Every IPv6 prefix list, including prefix lists that do not have permit and deny condition statements, has an implicit deny any any statement as its last match condition.

Formal Specification

Checked prefix is cP and checked prefix length is cL.

Function PrefixIsEqual(P1, P2, L) compares the first L bits of two addresses P1 and P2 and returns TRUE if they are equal.

Case 1. A prefix-list entry is:

- P - prefix address
- L - prefix length
- ge - is not defined
- le - is not defined

The prefix cP/cL matches the prefix-list entry if PrefixIsEqual(cP,P,L) && cL == L

Case 2. An prefix-list entry is:

- P - prefix address
- L - prefix length
- ge - is defined
- le - is not defined

The prefix cP/cL matches the prefix-list entry if PrefixIsEqual(cP,P,L) && cL >= ge

Case 3. An prefix-list entry is:

- P - prefix address
- L - prefix length
- ge - is not defined
- le - is defined

The prefix cP/cL matches to the prefix-list entry if PrefixIsEqual(cP,P,L) && cL <= le

Case 4. An prefix-list entry is:

- P - prefix address
- L - prefix length
- ge - is defined
- le - is defined

The prefix cP/cL matches the prefix-list entry if PrefixIsEqual(cP,P,L) && ge <= cL <= le

Examples

Example 1. The following example denies all routes with a prefix of ::/0:

```
switchxxxxxx(config)# ipv6 prefix-list abc deny ::/0
```

Example 2. The following example permits the prefix 2002::/16:

```
switchxxxxxx(config)# ipv6 prefix-list abc permit 2002::/16
```

Example 3. The following example shows how to specify a group of prefixes to accept any prefixes from prefix 5F00::/48 up to and including prefix 5F00::/64:

```
switchxxxxxx(config)# ipv6 prefix-list abc permit 5F00::/48 le 64
```

Example 4. The following example denies prefix lengths greater than 64 bits in routes that have the prefix 2001:0DB8::/64:

```
switchxxxxxx(config)# ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
```

Example 5. The following example permits mask lengths from 32 to 64 bits in all address space:

```
switchxxxxxx(config)# ipv6 prefix-list abc permit ::/0 ge 32 le 64
```

Example 6. The following example denies mask lengths greater than 32 bits in all address space:

```
switchxxxxxx(config)# ipv6 prefix-list abc deny ::/0 ge 32
```

Example 7. The following example denies all routes with a prefix of 2002::/128:

```
switchxxxxxx(config)# ipv6 prefix-list abc deny 2002::/128
```

Example 8. The following example permits all routes with a prefix of ::/0:

```
switchxxxxxx(config)# ipv6 prefix-list abc permit ::/0
```

26.3. show ipv6 prefix-list

Use the `show ipv6 prefix-list` command in user EXEC or privileged EXEC mode. to display information about an IPv6 prefix list or IPv6 prefix list entries.

Syntax

- show ipv6 prefix-list [detail [list-name] | summary [list-name]]
- show ipv6 prefix-list list-name ipv6-prefix/prefix-length [longer | first-match]
- show ipv6 prefix-list list-name seq seq-num

Parameters

- detail | summary - Displays detailed or summarized information about all IPv6 prefix lists.
- list-name - Name of a specific IPv6 prefix list.
- ipv6-prefix - All prefix list entries for the specified IPv6 network. This argument must be in the form documented in RFC 4293 where the address is specified in hexadecimal using 16-bit values between colons.
- /prefix-length - Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
- longer - Displays all entries of an IPv6 prefix list that are more specific than the given ipv6-prefix/prefix-length values.
- first-match - Displays the entry of an IPv6 prefix list that matches the given ipv6-prefix/prefix-length values.
- seq seq-num - Sequence number of the IPv6 prefix list entry.

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

If the detail and summary keywords are omitted, the detail option is applied.

If the longer and first-match keywords are omitted, all entries of the specified prefix list that matches the given network/length are displayed.

Examples

Example 1. The following example shows the output of this command with the detail keyword:

```
switchxxxxxx# ipv6 prefix-list detail ipv6 prefix-list aggregate:
 count: 3, range entries: 2 seq 5 deny 3FFE:C00::/24 ge 25 (hit count: 568) seq
10 description The Default Action seq 15 permit ::/0 le 48 (hit count: 31310)
Field Descriptions
count - Number of entries in the list.
range entries - Number of entries with matching range.
seq - Entry number in the list.
permit, deny - Granting status.
description - Comment.
hit count - Number of matches for the prefix entry.
```

Example 2. The following example shows the output of the show ipv6 prefix-list command with the summary keyword:

```
switchxxxxxx# show ipv6 prefix-list summary ipv6 prefix-list aggregate: count:
2, range entries: 2
```

Example 3. The following example shows the output of the show ipv6 prefix-list command with the seq keyword:

```
switchxxxxxx# show ipv6 prefix-list bgp-in seq 15 seq 15 deny ::/1 (hit count:
0)
```

27. Link Aggregation Control Protocol (LACP)

27.1. lacp port-priority

To set the physical port priority, use the `lacp port-priority` Interface (Ethernet) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- lacp port-priority value
- no lacp port-priority

Parameters

- value - Specifies the port priority. (Range: 1–65535)

Default Configuration

The default port priority is 1.

Command Mode

Interface (Ethernet) Configuration mode

Example

The following example sets the priority of `te1/0/6`.

```
switchxxxxxx(config)# interface te1/0/6
switchxxxxxx(config-if)# lacp port-priority 247
```

27.2. lacp system-priority

To set the system priority, use the `lacp system-priority` Global Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- lacp system-priority value
- no lacp system-priority

Parameters

- value - Specifies the system priority value. (Range: 1–65535)

Default Configuration

The default system priority is 1.

Command Mode

Global Configuration mode

Example

The following example sets the system priority to 120.

```
switchxxxxxx(config)# lacp system-priority 120
```

27.3. lacp timeout

To assign an administrative LACP timeout to an interface, use the `lacp timeout` Interface (Ethernet) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- lacp timeout {long | short}
- no lacp timeout

Parameters

- long - Specifies the long timeout value.
- short - Specifies the short timeout value.

Default Configuration

The default port timeout value is Long.

Command Mode

Interface (Ethernet) Configuration mode

Example

The following example assigns a long administrative LACP timeout to `te1/0/6`.

```
switchxxxxxx(config)# interface te1/0/6
switchxxxxxx(config-if)# lacp timeout long
```

27.4. show lacp

To display LACP information for all Ethernet ports or for a specific Ethernet port, use the `show lacp` Privileged EXEC mode command.

Syntax

- show lacp interface-id [parameters | statistics | protocol-state]

Parameters

- interface-id - Specify an interface ID. The interface ID must be an Ethernet port
- parameters - (Optional) Displays parameters only.
- statistics - (Optional) Displays statistics only.
- protocol-state - (Optional) Displays protocol state only.

Command Mode

Privileged EXEC mode

Example

The following example displays LACP information for `te1/0/1`.

```
switchxxxxxx# show lacp ethernet te1/0/1
Port te1/0/1 LACP parameters:
Actor
 system priority: 1
 system mac addr: 00:00:12:34:56:78
 port Admin key: 30
 port Oper key: 30
 port Oper number: 21
```

```
 port Admin priority: 1
 port Oper priority: 1
 port Admin timeout: LONG
 port Oper timeout: LONG
 LACP Activity: ACTIVE
 Aggregation: AGGREGATABLE
 synchronization: FALSE
 collecting: FALSE
 distributing: FALSE
 expired: FALSE
Partner
 system priority: 0
 system mac addr: 00:00:00:00:00:00
 port Admin key: 0
 port Oper key: 0
 port Oper number: 0
 port Admin priority: 0
 port Oper priority: 0
 port Admin timeout: LONG
 port Oper timeout: LONG
 LACP Activity: PASSIVE
 Aggregation: AGGREGATABLE
 synchronization: FALSE
 collecting: FALSE
 distributing: FALSE
 expired: FALSE
Port te1/0/1 LACP Statistics:
 LACP PDUs sent: 2
 LACP PDUs received: 2
Port te1/0/1 LACP Protocol State:
LACP State Machines:
 Receive FSM: Port Disabled State
 Mux FSM: Detached State
Control Variables:
 BEGIN: FALSE
 LACP_Enabled: TRUE
 Ready_N: FALSE
 Selected: UNSELECTED
 Port_moved: FALSE
 NNT: FALSE
 Port_enabled: FALSE
Timer counters:
 periodic tx timer: 0
 current while timer: 0
 wait while timer: 0
```

27.5. show lacp port-channel

To display LACP information for a port-channel, use the `show lacp port-channel` Privileged EXEC mode command.

Syntax

- show lacp port-channel [port_channel_number]

Parameters

- port_channel_number - (Optional) Specifies the port-channel number.

Command Mode

Privileged EXEC mode

Example

The following example displays LACP information about port-channel 1.

```
switchxxxxxx# show lacp port-channel 1
Port-Channel 1:Port Type 1000 Ethernet
Actor
 System Priority: 1
 MAC Address: 000285:0E1C00
 Admin Key: 29
 Oper Key: 29
Partner
 System Priority: 0
 MAC Address: 00:00:00:00:00:00
 Oper Key: 14
```

28. Line Commands

28.1. autobaud

To configure the line for automatic baud rate detection (autobaud), use the `autobaud` command in Line Configuration mode.

Use the no form of this command to disable automatic baud rate detection.

Syntax

- autobaud
- no autobaud

Parameters

This command has no arguments or keywords.

Default Configuration

Automatic baud rate detection is enabled.

Command Mode

Line Configuration Mode

User Guidelines

When this command is enabled, it is activated as follows: connect the console to the device and press the Enter key twice. The device detects the baud rate automatically.

Note that if characters other than Enter are typed, wrong speed might be detected.

Example

The following example enables autobaud.

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# autobaud
```

28.2. exec-timeout

To set the session idle time interval, during which the system waits for user input before automatic logoff, use the `exec-timeout` Line Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- exec-timeout minutes [seconds]
- no exec-timeout

Parameters

- minutes - Specifies the number of minutes. (Range: 0-65535)
- seconds - (Optional) Specifies the number of seconds. (Range: 0-59)

Default Configuration

The default idle time interval is 10 minutes.

Command Mode

Line Configuration Mode

Example

The following example sets the telnet session idle time interval before automatic logoff to 20 minutes and 10 seconds.

```
switchxxxxxx(config)# line telnet
switchxxxxxx(config-line)# exec-timeout 20 10
```

28.3. line

To identify a specific line for configuration and enter the Line Configuration command mode, use the `line` Global Configuration mode command.

Syntax

- line {console | telnet | ssh}

Parameters

- console - Enters the terminal line mode.
- telnet - Configures the device as a virtual terminal for remote access (Telnet).
- ssh - Configures the device as a virtual terminal for secured remote access (SSH).

Command Mode

Global Configuration mode

Example

The following example configures the device as a virtual terminal for remote (Telnet) access.

```
switchxxxxxx(config)# line telnet
switchxxxxxx(config-line)#
```

28.4. speed

To set the line baud rate, use the `speed` command in Line Configuration mode.

To restore the default configuration, use the no form of this command.

Syntax

- speed bps
- no speed

Parameters

- bps - Specifies the baud rate in bits per second (bps). Possible values are 4800, 9600, 19200, 38400, 57600, and 115200.

Default Configuration

The default speed is 115200 bps.

Command Mode

Line Configuration Mode

User Guidelines

The configured speed is only applied when autobaud is disabled. This configuration applies to the current session only.

Example

The following example configures the line baud rate as 9600 bits per second.

```
switchxxxxxx(config-line)# speed 9600
```

28.5. show line

To display line parameters, use the `show line` Privileged EXEC mode command.

Syntax

- show line [console | telnet | ssh]

Parameters

- console - (Optional) Displays the console configuration.
- telnet - (Optional) Displays the Telnet configuration.
- ssh - (Optional) Displays the SSH configuration.

Default Configuration

If the line is not specified, all line configuration parameters are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays the line configuration.

```
switchxxxxxx# show line Console configuration:
Interactive timeout: Disabled
History: 10
Baudrate: 9600
Databits: 8
Parity: none
Stopbits: 1
Telnet configuration:
Telnet is enabled.
Interactive timeout: 10 minutes 10 seconds
History: 10 SSH configuration:
SSH is enabled.
Interactive timeout: 10 minutes 10 seconds
History: 10
```

29. Link Layer Discovery Protocol (LLDP) Commands

29.1. clear lldp table

To clear the neighbors table for all ports or for a specific port, use the `clear lldp table` command in Privileged EXEC mode.

Syntax

- clear lldp table [interface-id]

Parameters

- interface-id - (Optional) Specifies a port ID.

Default Configuration

If no interface is specified, the default is to clear the LLDP table for all ports.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# clear lldp table te1/0/1
```

29.2. lldp chassis-id

To configure the source of the chassis ID of the port, use the `lldp chassis-id` Global Configuration mode command. To restore the chassis ID source to default, use the no form of this command.

Syntax

- lldp chassis-id {mac-address | host-name}
- no lldp chassis-id

Parameters

- mac-address - Specifies the chassis ID to use the device MAC address.
- host-name - Specifies the chassis ID to use the device configured host name.

Default Configuration

MAC address.

Command Mode

Global Configuration mode

User Guidelines

The host name should be configured to be a unique value.

If the chassis ID configured to be used in LLDP packets is empty, LLDP uses the default chassis ID (specified above).

Example

The following example configures the chassis ID to be the MAC address.

```
switchxxxxxx(config)# lldp chassis-id mac-address
```

29.3. lldp hold-multiplier

To specify how long the receiving device holds a LLDP packet before discarding it, use the `lldp hold-multiplier` Global Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- lldp hold-multiplier number no lldp hold-multiplier

Parameters

- hold-multiplier number - Specifies the LLDP packet hold time interval as a multiple of the LLDP timer value (range: 2-10).

Default Configuration

The default LLDP hold multiplier is 4.

Command Mode

Global Configuration mode

User Guidelines

The actual Time-To-Live (TTL) value of LLDP frames is calculated by the following formula:

TTL = min(65535, LLDP-Timer * LLDP-hold-multiplier)

For example, if the value of the LLDP timer is 30 seconds, and the value of the

LLDP hold multiplier is 4, then the value 120 is encoded in the TTL field of the LLDP header.

Example

The following example sets the LLDP packet hold time interval to 90 seconds.

```
switchxxxxxx(config)# lldp timer 30
switchxxxxxx(config)# lldp hold-multiplier 3
```

29.4. lldp lldpdu

To define LLDP packet handling when LLDP is globally disabled, use the `lldp lldpdu` Global Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- lldp lldpdu {filtering | flooding}
- no lldp lldpdu

Parameters

- filtering - Specifies that when LLDP is globally disabled, LLDP packets are filtered (deleted).
- flooding - Specifies that when LLDP is globally disabled, LLDP packets are flooded (forwarded to all interfaces).

Default Configuration

LLDP packets are filtered when LLDP is globally disabled.

Command Mode

Global Configuration mode

User Guidelines

If the STP mode is MSTP, the LLDP packet handling mode cannot be set to flooding and vice versa.

- If LLDP is globally disabled, and the LLDP packet handling mode is flooding, LLDP packets are treated as data packets with the following exceptions: VLAN ingress rules are not applied to LLDP packets. The LLDP packets are trapped on all ports for which the STP state is Forwarding.
- Default deny-all rules are not applied to LLDP packets. VLAN egress rules are not applied to LLDP packets. The LLDP packets are flooded to all ports for which the STP state is Forwarding.
- LLDP packets are sent as untagged.

Example

The following example sets the LLDP packet handling mode to Flooding when LLDP is globally disabled.

```
switchxxxxxx(config)# lldp lldpdu flooding
```

29.5. lldp management-address

To specify the management address advertised by an interface, use the `lldp management-address` Interface (Ethernet) Configuration mode command. To stop advertising management address information, use the no form of this command.

Syntax

- lldp management-address {ip-address | none | automatic [interface-id]}
- no lldp management-address

Parameters

- ip-address - Specifies the static management address to advertise.
- none - Specifies that no address is advertised.
- automatic - Specifies that the software automatically selects a management address to advertise from all the IP addresses of the product. In case of multiple IP addresses, the software selects the lowest IP address among the dynamic IP addresses. If there are no dynamic addresses, the software selects the lowest IP address among the static IP addresses.
- automatic interface-id - Specifies that the software automatically selects a management address to advertise from the IP addresses that are configured on the interface ID. In case of multiple IP addresses, the software selects the lowest IP address among the dynamic IP addresses of the interface. If there are no dynamic addresses, the software selects the lowest IP address among the static IP addresses of the interface. The interface ID can be one of the following types: Ethernet port, port-channel or VLAN. Note that if the port or port- channel are members in a VLAN that has an IP address, that address is not included because the address is associated with the VLAN.

Default Configuration

No IP address is advertised.

The default advertisement is automatic.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

Each port can advertise one IP address.

Example

The following example sets the LLDP management address advertisement mode to automatic on te1/0/2.

```
switchxxxxxx(config)# interface te1/0/2
switchxxxxxx(config-if)# lldp management-address automatic
```

29.6. lldp med

To enable or disable LLDP Media Endpoint Discovery (MED) on a port, use the `lldp med` Interface (Ethernet) Configuration mode command. To return to the default state, use the no form of this command.

Syntax

- lldp med {enable [tlv … tlv4] | disable}
- no lldp med

Parameters

- enable - Enable LLDP MED
- tlv - Specifies the TLV that should be included. Available TLVs are: Network-Policy, Location, and POE-PSE, Inventory. The Capabilities TLV is always included if LLDP-MED is enabled.
- disable - Disable LLDP MED on the port

Default Configuration

Enabled with network-policy TLV

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

It is possible to manage 8 locations with up to 450 neighbors.

Example

The following example enables LLDP MED with the location TLV on te1/0/3.

```
switchxxxxxx(config)# interface te1/0/3
switchxxxxxx(config-if)# lldp med enable location
```

29.7. lldp med notifications topology-change

To enable sending LLDP MED topology change notifications on a port, use the `lldp med notifications topology-change` Interface (Ethernet) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- lldp med notifications topology-change {enable | disable}
- no lldp med notifications topology-change

Parameters

- enable - Enables sending LLDP MED topology change notifications.
- disable - Disables sending LLDP MED topology change notifications.

Default Configuration

Disable is the default.

Command Mode

Interface (Ethernet) Configuration mode

Example

The following example enables sending LLDP MED topology change notifications on `te1/0/2`.

```
switchxxxxxx(config)# interface te1/0/2
switchxxxxxx(config-if)# lldp med notifications topology-change enable
```

29.8. lldp med fast-start repeat-count

When a port comes up, LLDP can send packets more quickly than usual using its fast-start mechanism.

To configure the number of packets that is sent during the activation of the fast start mechanism, use the `lldp med fast-start repeat-count` Global Configuration mode command. To return to default, use the no form of this command.

Syntax

- lldp med fast-start repeat-count number
- no lldp med fast-start repeat-count

Parameters

- repeat-count number - Specifies the number of times the fast start LLDPDU is being sent during the activation of the fast start mechanism. The range is 1-10.

Default Configuration

3

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# lldp med fast-start repeat-count 4
```

29.9. lldp med location

To configure the location information for the LLDP Media Endpoint Discovery (MED) for a port, use the `lldp med location` Interface (Ethernet) Configuration mode command. To delete location information for a port, use the no form of this command.

Syntax

- lldp med location {{coordinate data} | {civic-address data} | {ecs-elin data}}
- no lldp med location {coordinate | civic-address | ecs-elin}

Parameters

- coordinate data - Specifies the location data as coordinates in hexadecimal format.
- civic-address data - Specifies the location data as a civic address in hexadecimal format.
- ecs-elin data - Specifies the location data as an Emergency Call Service Emergency Location Identification Number (ECS ELIN) in hexadecimal format.
- data - Specifies the location data in the format defined in ANSI/TIA 1057: dotted hexadecimal data: Each byte in a hexadecimal character string is two hexadecimal digits. Bytes are separated by a period or colon. (Length: coordinate: 16 bytes. Civic-address: 6-160 bytes. Ecs-elin: 10-25 bytes)

Default Configuration

The location is not configured.

Command Mode

Interface (Ethernet) Configuration mode

Example

The following example configures the LLDP MED location information on te1/0/2 as a civic address.

```
switchxxxxxx(config)# interface te1/0/2
switchxxxxxx(config-if)# lldp med location civic-address 616263646566
```

29.10. lldp med network-policy (global)

To define a LLDP MED network policy, use the `lldp med network-policy` Global Configuration mode command.For voice applications, it is simpler to use `lldp med network-policy voice auto`.

The lldp med network-policy command creates the network policy, which is attached to a port by `lldp med network-policy (interface)`.

The network policy defines how LLDP packets are constructed.

To remove LLDP MED network policy, use the no form of this command.

Syntax

- lldp med network-policy number application [vlan vlan-id] [vlan-type {tagged | untagged}] [up priority] [dscp value]
- no lldp med network-policy number

Parameters

- number - Network policy sequential number. The range is 1-32.
- application - The name or the number of the primary function of the application defined for this network policy. Available application names are:
  - voice
  - voice-signaling
  - guest-voice
  - guest-voice-signaling
  - softphone-voice
  - video-conferencing
  - streaming-video - video-signaling.

- vlan vlan-id - (Optional) VLAN identifier for the application.
- vlan-type - (Optional) Specifies if the application is using a tagged or an untagged VLAN.
- up priority - (Optional) User Priority (Layer 2 priority) to be used for the specified application.
- dscp value - (Optional) DSCP value to be used for the specified application.

Default Configuration

No network policy is defined.

Command Mode

Global Configuration mode

User Guidelines

Use the `lldp med network-policy` Interface Configuration command to attach a network policy to a port.

Up to 32 network policies can be defined.

Example

This example creates a network policy for the voice-signal application and attaches it to port 1. LLDP packets sent on port 1 will contain the information defined in the network policy.

```
switchxxxxxx(config)# lldp med network-policy 1 voice-signaling vlan 1 vlan-type
untagged up 1 dscp 2
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# lldp med network-policy add 1
```

29.11. lldp med network-policy (interface)

To attach or remove an LLDP MED network policy on a port, use the `lldp med network-policy` Interface (Ethernet) Configuration mode command. Network policies are created in `lldp med network-policy (global)`.

To remove all the LLDP MED network policies from the port, use the no form of this command.

Syntax

- lldp med network-policy {add | remove} number
- no lldp med network-policy number

Parameters

- add/remove number - Attaches/removes the specified network policy to the interface.
- number - Specifies the network policy sequential number. The range is 1-32

Default Configuration

No network policy is attached to the interface.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

For each port, only one network policy per application (voice, voice-signaling, etc.) can be defined.

Example

This example creates a network policy for the voice-signally application and attaches it to port 1. LLDP packets sent on port 1 will contain the information defined in the network policy.

```
switchxxxxxx(config)# lldp med network-policy 1 voice-signaling vlan 1 vlan-type
untagged up 1 dscp 2
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# lldp med network-policy add 1
```

29.12. lldp med network-policy voice auto

A network policy for voice LLDP packets can be created by using the `lldp med network-policy (global)`. The lldp med network-policy voice auto Global Configuration mode is simpler in that it uses the configuration of the Voice application to create the network policy instead of the user having to manually configure it.

This command generates an LLDP MED network policy for voice, if the voice VLAN operation mode is auto voice VLAN. The voice VLAN, 802.1p priority, and the DSCP of the voice VLAN are used in the policy.

To disable this mode, use the no form of this command.

The network policy is attached automatically to the voice VLAN.

Syntax

- lldp med network-policy voice auto
- no lldp med network-policy voice auto

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Global Configuration mode

User Guidelines

In Auto mode, the Voice VLAN feature determines on which interfaces to advertise the network policy TLV with application type voice, and controls the parameters of that TLV.

To enable the auto generation of a network policy based on the auto voice VLAN, there must be no manually pre-configured network policies for the voice application

In Auto mode, you cannot manually define a network policy for the voice application using the `lldp med network-policy (global)` command.

Example

```
switchxxxxxx(config)# lldp med network-policy voice auto
```

29.13. lldp notifications

To enable/disable sending LLDP notifications on an interface, use the `lldp notifications` Interface (Ethernet) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- lldp notifications {enable | disable}
- no lldp notifications

Parameters

- enable - Enables sending LLDP notifications.
- disable - Disables sending LLDP notifications.

Default Configuration

Disabled.

Command Mode

Interface (Ethernet) Configuration mode

Example

The following example enables sending LLDP notifications on te1/0/1.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# lldp notifications enable
```

29.14. lldp notifications interval

To configure the maximum transmission rate of LLDP notifications, use the `lldp notifications interval` Global Configuration mode command. To return to the default, use the no form of this command.

Syntax

- lldp notifications interval seconds
- no lldp notifications interval

Parameters

- interval seconds - The device does not send more than a single notification in the indicated period (range: 5–3600).

Default Configuration

5 seconds

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# lldp notifications interval 10
```

29.15. lldp optional-tlv

To specify which optional TLVs are transmitted, use the `lldp optional-tlv` Interface (Ethernet) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- lldp optional-tlv tlv [tlv2 … tlv5 | none]

Parameters

- tlv - Specifies the TLVs to be included. Available optional TLVs are: port-desc, sys-name, sys-desc, sys-cap, 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size, Power-via-MDI , 4-wirePower-via-MDI.
- none - (Optional) Clear all optional TLVs from the interface.

If the 802.1 protocol is selected, see the command below.

Default Configuration

The following TLV are transmitted:

- sys-name
- sys-cap

Command Mode

Interface (Ethernet) Configuration mode

Example

The following example specifies that the port description TLV is transmitted on te1/0/2.

```
switchxxxxxx(config)# interface te1/0/2
switchxxxxxx(config-if)# lldp optional-tlv port-desc
```

29.16. lldp optional-tlv 802.1

To specify whether to transmit the 802.1 TLV, use the `lldp optional-tlv 802.1` Interface (Ethernet) Configuration mode command. To revert to the default setting, use the no form of this command.

Syntax

- lldp optional-tlv 802.1 pvid {enable | disable} - The PVID is advertised or not advertised.
- no lldp optional-tlv 802.1 pvid - The PVID advertise state is returned to default.
- lldp optional-tlv 802.1 ppvid add ppvid - The Protocol Port VLAN ID (PPVID) is advertised. The PPVID is the PVID that is used depending on the packet’s protocol. lldp optional-tlv 802.1 ppvid remove ppvid - The PPVID is not advertised.
- lldp optional-tlv 802.1 vlan add vlan-id - This vlan-id is advertised. lldp optional-tlv 802.1 vlan remove vlan-id - This vlan-id is not advertised.
- lldp optional-tlv 802.1 protocol add {stp | rstp | mstp | pause | 802.1x | lacp | gvrp} - The protocols selected are advertised.
- lldp optional-tlv 802.1 protocol remove {stp | rstp | mstp | pause | 802.1x | lacp | gvrp} - The protocols selected are not advertised.

Parameters

- lldp optional-tlv 802.1 pvid {enable | disable} - Advertises or stop advertize the PVID of the port.
- lldp optional-tlv 802.1 ppvid add/remove ppvid - Adds/removes PPVID for advertising. (range: 0–4094). PPVID = 0 indicates that the port is not capable of supporting port and protocol VLANs and/or the port is not enabled with any protocol VLANs.
- add/remove vlan-id - Adds/removes VLAN for advertising (range: 0–4094).
- add/remove {stp | rstp | mstp | pause | 802.1x | lacp | gvrp} - Add specifies to advertise the specified protocols; remove specifies not to advertise the specified protocol.

Default Configuration

The following 802.1 TLV is transmitted:

Command Mode

Interface (Ethernet) Configuration mode

Example

```
switchxxxxxx(config)# lldp optional-tlv 802.1 protocol add stp
```

29.17. lldp run

To enable LLDP, use the `lldp run` Global Configuration mode command. To disable LLDP, use the no form of this command.

Syntax

- lldp run
- no lldp run

Parameters

This command has no arguments or keywords.

Default Configuration

Enabled

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# lldp run
```

29.18. lldp receive

To enable receiving LLDP on an interface, use the `lldp receive` Interface (Ethernet) Configuration mode command. To stop receiving LLDP on an Interface (Ethernet) Configuration mode interface, use the no form of this command.

Syntax

- lldp receive
- no lldp receive

Parameters

This command has no arguments or keywords.

Default Configuration

Enabled

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

LLDP manages LAG ports individually. LLDP data received through LAG ports is stored individually per port.

LLDP operation on a port is not dependent on the STP state of a port. I.e. LLDP frames are received on blocked ports.

If a port is controlled by 802.1x, LLDP operates only if the port is authorized.

Example

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# lldp receive
```

29.19. lldp reinit

To specify the minimum time an LLDP port waits before reinitializing LLDP transmission, use the `lldp reinit` Global Configuration mode command. To revert to the default setting, use the no form of this command.

Syntax

- lldp reinit seconds
- no lldp reinit

Parameters

- reinit seconds - Specifies the minimum time in seconds an LLDP port waits before reinitializing LLDP transmission.(Range: 1–10)

Default Configuration

2 seconds

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# lldp reinit 4
```

29.20. lldp timer

To specify how often the software sends LLDP updates, use the `lldp timer` Global Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- lldp timer seconds
- no lldp timer

Parameters

- timer seconds - Specifies, in seconds, how often the software sends LLDP updates (range: 5-32768 seconds).

Default Configuration

30 seconds.

Command Mode

Global Configuration mode

Example

The following example sets the interval for sending LLDP updates to 60 seconds.

```
switchxxxxxx(config)# lldp timer 60
```

29.21. lldp transmit

To enable transmitting LLDP on an interface. Use the no form of this command to stop transmitting LLDP on an interface, use the `lldp transmit` Interface (Ethernet) Configuration mode command.

Syntax

- lldp transmit
- no lldp transmit

Parameters

This command has no arguments or keywords.

Default Configuration

Enabled

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

LLDP manages LAG ports individually. LLDP sends separate advertisements on each port in a LAG.

LLDP operation on a port is not dependent on the STP state of a port. I.e. LLDP frames are sent on blocked ports.

If a port is controlled by 802.1x, LLDP operates only if the port is authorized.

Example

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# lldp transmit
```

29.22. lldp tx-delay

To set the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB, use the `lldp tx-delay` Global Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- lldp tx-delay seconds
- no lldp tx-delay

Parameters

- tx-delay seconds - Specifies the delay in seconds between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB (range: 1-8192 seconds).

Default Configuration

The default LLDP frame transmission delay is 2 seconds.

Command Mode

Global Configuration mode

User Guidelines

It is recommended that the tx-delay be less than 25% of the LLDP timer interval.

Example

The following example sets the LLDP transmission delay to 10 seconds.

```
switchxxxxxx(config)# lldp tx-delay 10
```

29.23. show lldp configuration

To display the LLDP configuration for all ports or for a specific port, use the `show lldp configuration` Privileged EXEC mode command.

Syntax

- show lldp configuration [interface-id | detailed]

Parameters

- interface-id - (Optional) Specifies the port ID.
- detailed - (Optional) Displays information for non-present ports in addition to present ports.

Default Configuration

Display for all ports. If detailed is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

Examples

Example 1 - Display LLDP configuration for all ports.

```
switchxxxxxx# show lldp configuration
State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
Notifications interval: 5 seconds
LLDP packets handling: Filtering
Port State Optional TLVs Address Notifications
-------- ----- -------------- ----------- ------------
te1/0/1 RX,TX PD, SN, SD, SC , 4W 172.16.1.1 Disabled
te1/0/2 TX PD, SN 172.16.1.1 Disabled
te1/0/3 RX,TX PD, SN, SD, SC None Disabled
te1/0/4 RX,TX D, SN, SD, SC automatic Disabled
```

Example 2 - Display LLDP configuration for port 1.

```
switchxxxxxx# show lldp configuration te1/0/1
 State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
Notifications interval: 5 seconds
LLDP packets handling: Filtering
```

```
Chassis ID: mac-address
Port State Optional TLVs Address Notifications ---- ---------- -------------- --
--------- ----------te1/0/1 RX, TX PD, SN, SD, SC, 4W 72.16.1.1 Disabled
802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size
802.1 optional TLVs
PVID: Enabled
PPVIDs: 0, 1, 92
VLANs: 1, 92
Protocols: 802.1x
```

The following table describes the significant fields shown in the display:

Field	Description
Timer	The time interval between LLDP updates.
Hold multiplier	The amount of time (as a multiple of the timer interval) that the receiving device holds a LLDP packet before discarding it.
Reinit timer	The minimum time interval an LLDP port waits before re-initializing an LLDP transmission.
Field	Description
Tx delay	The delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB.
Port	The port number.
State	The port’s LLDP state.
Optional TLVs	Optional TLVs that are advertised. Possible values are: PD - Port description SN - System name SD - System description SC - System capabilities 4W - 4 wire spare pair capability
Address	The management address that is advertised.
Notifications	Indicates whether LLDP notifications are enabled or disabled.
PVID	Port VLAN ID advertised.
PPVID	Protocol Port VLAN ID advertised.
Protocols	

29.24. show lldp local

To display the LLDP information that is advertised from a specific port, use the `show lldp local` Privileged EXEC mode command.

Syntax

- show lldp local interface-id

Parameters

- Interface-id - (Optional) Specifies a port ID.

Default Configuration

If no port ID is entered, the command displays information for all ports.

Command Mode

Privileged EXEC mode

Example

The following examples display LLDP information that is advertised from `te1/0/1` and 2.

```
switchxxxxxx# show lldp local te1/0/1
Device ID: 0060.704C.73FF
Port ID: te1/0/1
Capabilities: Bridge
System Name: ts-7800-1 System description:
Port description:
Management address: 172.16.1.8
802.3 MAC/PHY Configuration/Status
Auto-negotiation support: Supported
Auto-negotiation status: Enabled
Auto-negotiation Advertised Capabilities: 100BASE-TX full duplex, 1000BASE-T
full duplex
Operational MAU type: 1000BaseTFD
802.3 Link Aggregation
Aggregation capability: Capable of being aggregated
Aggregation status: Not currently in aggregation
Aggregation port ID: 1
802.3 Maximum Frame Size: 1522
Power Type: Type 1 PSE
Power Source: Primary Power Source
Power Priority: Unknown
PSE Allocated Power Value: 30
4-Pair POE supported: Yes
Spare Pair Detection/Classification required: Yes
PD Spare Pair Desired State: Enabled
802.3 EEE
Local Tx: 30 usec
Local Rx: 25 usec
Remote Tx Echo: 30 usec
Remote Rx Echo: 25 usec
802.1 PVID: 1
802.1 PPVID: 2 supported, enabled
802.1 VLAN: 2 (VLAN2)
802.1 Protocol: 88 08 00 01 (PAUSE)
LLDP-MED capabilities: Network Policy, Location Identification
LLDP-MED Device type: Network Connectivity
LLDP-MED Network policy
Application type: Voice
Flags: Tagged VLAN
VLAN ID: 2
Layer 2 priority: 0
DSCP: 0
LLDP-MED Power over Ethernet
```

```
Device Type: Power Sourcing Entity
Power source: Primary Power Source
Power priority: High
Power value: 9.6 Watts
LLDP-MED Location
Coordinates: 54:53:c1:f7:51:57:50:ba:5b:97:27:80:00:00:67:01
Hardware Revision: B1
Firmware Revision: A1
Software Revision: 3.8
Serial number: 7978399
Manufacturer name: Manufacturer
Model name: Model 1 Asset ID: Asset 123
switchxxxxxx# show lldp local te1/0/2 LLDP is disabled.
```

29.25. show lldp local tlvs-overloading

When an LLDP packet contains too much information for one packet, this is called overloading. To display the status of TLVs overloading of the LLDP on all ports or on a specific port, use the `show lldp local tlvs-overloading` EXEC mode command.

Syntax

- show lldp local tlvs-overloading [interface-id]

Parameters

- interface-id - (Optional) Specifies a port ID.

Default Configuration

If no port ID is entered, the command displays information for all ports.

Command Mode

User EXEC mode

User Guidelines

The command calculates the overloading status of the current LLDP configuration, and not for the last LLDP packet that was sent.

Example

```
switchxxxxxx# show lldp local tlvs-overloading te1/0/1
TLVs Group Bytes Status
------------ ------ --------------
Mandatory 31 Transmitted
LLDP-MED Capabilities 9 Transmitted
LLDP-MED Location 200 Transmitted 802.1 1360 Overloading
Total: 1600 bytes
Left: 100 bytes
```

29.26. show lldp med configuration

To display the LLDP Media Endpoint Discovery (MED) configuration for all ports or for a specific port, use the `show lldp med configuration` Privileged EXEC mode command.

Syntax

- show lldp med configuration [interface-id | detailed]

Parameters

- interface-id - (Optional) Specifies the port ID.
- detailed - (Optional) Displays information for non-present ports in addition to present ports.

Default Configuration

If no port ID is entered, the command displays information for all ports. If detailed is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

Examples

Example 1 - The following example displays the LLDP MED configuration for all interfaces.

```
switchxxxxxx# show lldp med configuration
Fast Start Repeat Count: 4.
lldp med network-policy voice: manual
Network policy 1
-------------------
Application type: voiceSignaling
VLAN ID: 1 untagged
Layer 2 priority: 0
DSCP: 0
Port Capabilities Network Policy Location Notifications Inventory
------ -------------- -------------- ---------- ------------- --------
te1/0/1 Yes Yes Yes Enabled Yes
te1/0/2 Yes Yes No Enabled No
te1/0/3 No No No Enabled No
```

Example 2 - The following example displays the LLDP MED configuration for te1/0/1.

```
switchxxxxxx# show lldp med configuration te1/0/1
Port Capabilities Network Policy Location Notifications Inventory
------- -------------- ---------------- --------- ---------- --------
te1/0/1 Yes Yes Yes Enabled Yes
Network policies:
Location:
Civic-address: 61:62:63:64:65:66
```

29.27. show lldp neighbors

To display information about neighboring devices discovered using LLDP, use the `show lldp neighbors` Privileged EXEC mode command. The information can be displayed for all ports or for a specific port.

Syntax

- show lldp neighbors [interface-id]

Parameters

- interface-id - (Optional) Specifies a port ID.

Default Configuration

If no port ID is entered, the command displays information for all ports.

Command Mode

Privileged EXEC mode

User Guidelines

TLV value that cannot be displayed as an ASCII string is displayed as an hexadecimal string.

Examples

Example 1 - The following example displays information about neighboring devices discovered using LLDP on all ports on which LLDP is enabled and who are up.

Location information, if it exists, is also displayed.

```
switchxxxxxx# show lldp neighbors
System capability legend:
- Bridge; R - Router; W - Wlan Access Point; T - telephone;
D - DOCSIS Cable Device; H - Host; r - Repeater;
TP - Two Ports MAC Relay; S - S-VLAN; C - C-VLAN; O - Other
Port Device ID Port ID System Name Capabilities TTL ----- --------------- ------
-- ---------- ----------- ---te1/0/1 00:00:00:11:11:11 te1/0/1 ts-7800-2 B 90
te1/0/1 00:00:00:11:11:11 te1/0/1 ts-7800-2 B 90 te1/0/2 00:00:26:08:13:24
te1/0/3 ts-7900-1 B,R 90 te1/0/3 00:00:26:08:13:24 te1/0/2 ts-7900-2 W 90
Example 2 - The following example displays information about neighboring devices
discovered using LLDP on port 1.
switchxxxxxx# show lldp neighbors te1/0/1
Device ID: 00:00:00:11:11:11
Port ID: te1/0/1
System Name: ts-7800-2
Capabilities: B System description:
Port description:
Management address: 172.16.1.1
Time To Live: 90 seconds 802.3 MAC/PHY Configuration/Status
Auto-negotiation support: Supported.
Auto-negotiation status: Enabled.
Auto-negotiation Advertised Capabilities: 100BASE-TX full duplex, 1000BASE-T
full duplex.
Operational MAU type: 1000BaseTFD
802.3 Power via MDI
MDI Power support Port Class: PD
PSE MDI Power Support: Not Supported
PSE MDI Power State: Not Enabled
PSE power pair control ability: Not supported.
PSE Power Pair: Signal
PSE Power class: 1
Power Type: Type 1 PSE
Power Source: Primary Power Source
Power Priority: Unknown
PD Requested Power Value: 30
4-Pair POE supported: Yes
Spare Pair Detection/Classification required: Yes
PD Spare Pair Desired State: Enabled
PD Spare Pair Operational State: Enabled
802.3 Link Aggregation
Aggregation capability: Capable of being aggregated
Aggregation status: Not currently in aggregation
Aggregation port ID: 1
802.3 Maximum Frame Size: 1522
```

```
802.3 EEE
Remote Tx: 25 usec
Remote Rx: 30 usec
Local Tx Echo: 30 usec
Local Rx Echo: 25 usec
802.1 PVID: 1
802.1 PPVID: 2 supported, enabled
802.1 VLAN: 2(VLAN2)
802.1 Protocol: 88 8E 01
LLDP-MED capabilities: Network Policy.
LLDP-MED Device type: Endpoint class 2.
LLDP-MED Network policy
Application type: Voice
Flags: Unknown policy
VLAN ID: 0
Layer 2 priority: 0
DSCP: 0
LLDP-MED Power over Ethernet
Device Type: Power Device
Power source: Primary power
Power priority: High
Power value: 9.6 Watts
Hardware revision: 2.1
Firmware revision: 2.3
Software revision: 2.7.1
Serial number: LM759846587
Manufacturer name: VP
Model name: TR12
Asset ID: 9
LLDP-MED Location
Coordinates: 54:53:c1:f7:51:57:50:ba:5b:97:27:80:00:00:67:01
```

The following table describes significant LLDP fields shown in the display:

Field	Description
Port	The port number.
Device ID	The neighbor device’s configured ID (name) or MAC address.
Port ID	The neighbor device’s port ID.
System name	The neighbor device’s administratively assigned name.
Capabilities	The capabilities discovered on the neighbor device. Possible values are: B - Bridge R - Router W - WLAN Access Point T - Telephone D - DOCSIS cable device H - Host r - Repeater O - Other
System description	The neighbor device’s system description.
Port description	The neighbor device’s port description.

Management address	The neighbor device's management address.
Auto-negotiation support	The auto-negotiation support status on the port. (supported or not supported)
Auto-negotiation status	The active status of auto-negotiation on the port. (enabled or disabled)
Auto-negotiation Advertised Capabilities	The port speed/duplex/flow-control capabilities advertised by the auto-negotiation.
Operational MAU type	The port MAU type.
Power Source	The power source utilized by a PSE or PD device. A PSE device advertises its power capability. The possible values are: Primary power source, Backup power source. Unknown Power source, PSE and local power source, Local Only power source and PSE only power source.
LLDP MED	
Capabilities	The sender's LLDP-MED capabilities.
Device type	The device type. Indicates whether the sender is a Network Connectivity Device or Endpoint Device, and if an Endpoint, to which Endpoint Class it belongs.
LLDP MED - Network Policy	
Application type	The primary function of the application defined for this network policy.
Flags	Flags. The possible values are: ▪ Unknown policy: Policy is required by the device, but is currently unknown. ▪ Tagged VLAN: The specified application type is using a tagged VLAN. ▪ Untagged VLAN: The specified application type is using an Untagged VLAN.
VLAN ID	The VLAN identifier for the application.
Layer 2 priority	The Layer 2 priority used for the specified application.
DSCP	The DSCP value used for the specified application.
LLDP MED - Power Over Ethernet	
Power type	The device power type. The possible values are: Power Sourcing Entity (PSE) or Power Device (PD).
Power Source	The power source utilized by a PSE or PD device. A PSE device advertises its power capability. The possible values are: Primary power source and Backup power source. A PD device advertises

	its power source. The possible values are: Primary power, Local power, Primary and Local power.
Power priority	The PD device priority. A PSE device advertises the power priority configured for the port. A PD device advertises the power priority configured for the device. The possible values are: Critical, High and Low.
Power value	The total power in watts required by a PD device from a PSE device, or the total power a PSE device is capable of sourcing over a maximum length cable based on its current configuration.
LLDP MED - Location	
Coordinates, Civic	The location information raw data. address, ECS ELIN.

29.28. show lldp statistics

To display LLDP statistics on all ports or a specific port, use the `show lldp statistics` EXEC mode command.

Syntax

- show lldp statistics [interface-id | detailed]

Parameters

- interface-id - (Optional) Specifies the port ID.
- detailed - (Optional) Displays information for non-present ports in addition to present ports.

Default Configuration

If no port ID is entered, the command displays information for all ports. If detailed is not used, only present ports are displayed.

Command Mode

User EXEC mode

Example

```
switchxxxxxx# show lldp statistics
Tables Last Change Time: 14-Oct-2010 32:08:18
Tables Inserts: 26
Tables Deletes: 2
Tables Dropped: 0
Tables Ageouts: 1
 TX Frames RX Frame RX TLVs RX Ageouts
Port Total Total Discarded Errors Discarded Unrecognized Total
----- ---- ----- --------- --------- --------- --------- ------------
te1/0/1 730 850 0 0 0   0 0
te1/0/2 0 0 0 0 0       0 0
te1/0/3 730 0 0 0 0     0 0
te1/0/4 0 0 0 0 0       0 0
```

The following table describes significant LLDP fields shown in the display:

Field	Description

Port	The port number.
Device ID	The neighbor device’s configured ID (name) or MAC address.
Port ID	The neighbor device’s port ID.
System name	The neighbor device’s administratively assigned name.
Capabilities	The capabilities discovered on the neighbor device. Possible values are: B - Bridge R - Router W - WLAN Access Point T - Telephone D - DOCSIS cable device H - Host r - Repeater O - Other
System description	The neighbor device’s system description.
Port description	The neighbor device’s port description.
Management address	The neighbor device’s management address.
Auto-negotiation support	The auto-negotiation support status on the port. (Supported or Not Supported)
Auto-negotiation status	The active status of auto-negotiation on the port. (Enabled or Disabled)
Auto-negotiation Capabilities	The port speed/duplex/flow-control capabilities Advertised advertised by the auto-negotiation
Operational MAU type	The port MAU type.
LLDP MED	
Capabilities	The sender's LLDP-MED capabilities.
Device type	The device type. Indicates whether the sender is a Network Connectivity Device or Endpoint Device, and if an Endpoint, to which Endpoint Class it belongs.
LLDP MED - Network Policy	
Application type	The primary function of the application defined for this network policy.
Flags	Flags. The possible values are: ■ Unknown policy: Policy is required by the device, but is currently unknown. ■ Tagged VLAN: The specified application type is using a Tagged VLAN. ■ Untagged VLAN: The specified application type is using an Untagged VLAN.

VLAN ID	The VLAN identifier for the application.
Layer 2 priority	The Layer 2 priority used for the specified application.
DSCP	The DSCP value used for the specified application.
LLDP MED - Power Over Ethernet	
Power type	The device power type. The possible values are: Power Sourcing Entity (PSE) or Power Device (PD).
Power Source	The power source utilized by a PSE or PD device. A PSE device advertises its power capability. The possible values are: Primary power source and Backup power source. A PD device advertises its power source. The possible values are: Primary power, Local power, Primary and Local power.
Power priority	The PD device priority. A PSE device advertises the power priority configured for the port. A PD device advertises the power priority configured for the device. The possible values are: Critical, High and Low.
Power value	The total power in watts required by a PD device from a PSE device, or the total power a PSE device is capable of sourcing over a maximum length cable based on its current configuration.
LLDP MED - Location	
Coordinates, Civic	The location information raw data. address, ECS ELIN.

30. Loopback Detection Commands

30.1. loopback-detection enable (Global)

To enable the Loopback Detection (LBD) feature globally, use the `loopback-detection enable` Global Configuration mode command. To disable the Loopback Detection feature, use the no form of this command.

Syntax

- loopback-detection enable
- no loopback-detection enable

Parameters

This command has no arguments or keywords.

Default Configuration

Loopback Detection is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables the Loopback Detection feature globally. Use the `loopback-detection enable` Interface Configuration mode command to enable Loopback Detection on an interface.

Example

The following example enables the Loopback Detection feature on the device.

```
switchxxxxxx(config)# loopback-detection enable
```

30.2. loopback-detection enable (Interface)

To enable the Loopback Detection (LBD) feature on an interface, use the `loopback-detection enable` Interface (Ethernet, Port Channel) Configuration mode command. To disable the Loopback Detection feature on the interface, use the no form of this command.

Syntax

- loopback-detection enable
- no loopback-detection enable

Parameters

This command has no arguments or keywords.

Default Configuration

Loopback Detection is enabled on an interface.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

This command enables Loopback Detection on an interface. Use the `loopback-detection enable` Global Configuration command to enable Loopback Detection globally.

Example

The following example enables the Loopback Detection feature on port `te1/0/4`.

```
switchxxxxxx(config)# interface te1/0/4
switchxxxxxx(config-if)# loopback-detection enable
```

30.3. loopback-detection interval

To set the time interval between LBD packets, use the `loopback-detection interval` Global Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- loopback-detection interval seconds
- no loopback-detection interval

Parameters

- seconds - Specifies the time interval in seconds between LBD packets. (Range: 10–60 seconds)

Default Configuration

The default time interval between LBD packets is `30` seconds.

Command Mode

Global Configuration mode

Example

The following example sets the time interval between LBD packets to 45 seconds.

```
switchxxxxxx(config)# loopback-detection interval 45
```

30.4. show loopback-detection

To display information about Loopback Detection, use the `show loopback-detection` Privileged EXEC mode command.

Syntax

- show loopback-detection [interface-id | detailed]

Parameters

- interface-id - (Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.
- detailed - (Optional) Displays information for non-present ports in addition to present ports. If this is not set, the default is to display all present ports.

Default Configuration

All ports are displayed. If detailed is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

User Guidelines

Operational status of `Active` indicates the following conditions are meet:

- Loopback is globally enabled.
- Loopback is enabled on the interface.
- Interface operational state of the interface is up.
- Interface STP state is Forwarding or STP state is disabled.

Operational status of `LoopDetected` indicates that the interface entered errDisabled state (see `set interface active` or `errdisable recovery cause` for more information).

Operational status of Inactive indicates that loopback detection is not actively attempting to detect loops, i.e. the `Active` status conditions are not meet.

Example

The following example displays information about the status of Loopback Detection.

```
Console# show loopback-detection
Loopback detection: Enabled
LBD packets interval: 30 Seconds
Interface Loopback Detection Loopback Detection
 Admin State Operational State
-------- ------------------ -----------------
te1/0/1 Enabled Active
te1/0/2 Enabled LoopDetected
te1/0/3 Enabled Inactive
te1/0/4 Disabled Inactive
```

31. Macro Commands

31.1. macro name

Use the `macro name` Global Configuration mode command to define a macro. There are two types of macros that can be defined:

- Global macros define a group of CLI commands that can be run at any time.
- Smartport macros are associated with Smartport types. For each Smartport macro there must be an anti macro (a macro whose name is concatenated with no_). The anti macro reverses the action of the macro.

If a macro with this name already exists, it overrides the previously-defined one.

Use the no form of this command to delete the macro definition.

Syntax

- macro name macro-name
- no macro name [macro-name]

Parameters

- macro-name - Name of the macro. Macro names are case sensitive.

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

A macro is a script that contains CLI commands and is assigned a name by the user. It can contain up to 3000 characters and 200 lines.

Keywords

Macros may contain keywords (parameters). The following describes these keywords:

- A macro can contain up to three keywords.
- All matching occurrences of the keyword are replaced by the corresponding value specified in the macro command.
- Keyword matching is case-sensitive
- Applying a macro with keywords does not change the state of the original macro definition.

User Feedback

The behavior of a macro command requiring user feedback is the same as if the command is entered from terminal: it sends its prompt to the terminal and accepts the user reply.

Creating a Macro

Use the following guidelines to create a macro:

- Use macro name to create the macro with the specified name.
- Enter one macro command per line.
- Use the @ character to end the macro.
- Use the # character at the beginning of a line to enter a comment in the macro.

In addition, # is used to identify certain preprocessor commands that can only be used within a macro. There are two possible preprocessor commands:

- #macro key description - Each macro can be configured with up to 3 keyword/description pairs. The keywords and descriptions are displayed in the GUI pages when the macro is displayed.

The Syntax for this preprocessor command is as follows:

```
#macro key description $keyword1 description1 $keyword2 description2 $keyword3
description3
```

A keyword must be prefixed with '$'.

- #macro keywords - This instruction enables the device to display the keywords as part of the CLI help. It accepts up to 3 keywords. The command creates a CLI help string with the keywords for the macro. The help string will be displayed if help on the macro is requested from the macro and macro global commands. The GUI also uses the keywords specified in the command as the parameter names for the macro. See Example 2 and 3 below for a description of how this command is used in the CLI.

The Syntax for this preprocessor command is as follows: #macro keywords $keyword1 $keyword2 $keyword3 where $keywordn is the name of the keyword.

Editing a Macro

Macros cannot be edited. Modify a macro by creating a new macro with the same name as the existing macro. The newer macro overwrites the existing macro.

Scope of Macro

It is important to consider the scope of any user-defined macro. Because of the potential hazards of applying unintended configurations, do not change configuration modes within the macro by using commands such as exit, end, or interface interface-id. With a few exceptions, there are other ways of executing macros in the various configuration modes. Macros may be executed in Privileged Exec mode, Global Configuration mode, and Interface Configuration mode (when the interface is NOT a VLAN.)

Examples

Example 1 -The following example shows how to create a macro that configures the duplex mode of a port.

```
switchxxxxxx(config)# macro name dup
Enter macro commands one per line. End with the character '@'.
#macro description dup duplex full negotiation
@
```

Example 2 -The following example shows how to create a macro with the parameters: DUPLEX and SPEED. When the macro is run, the values of DUPLEX and SPEED must be provided by the user. The #macro keywords command enables the user to receive help for the macro as shown in Example 3.

```
switchxxxxxx(config)# macro name duplex
Enter macro commands one per line. End with the character '@'.
duplex $DUPLEX no negotiation speed $SPEED
#macro keywords $DUPLEX $SPEED
@
```

Example 3 -The following example shows how to display the keywords using the help character ? (as defined by the #macro keywords command above) and then run the macro on the port. The #macro keywords command entered in the macro definition enables the user to receive help for the macro, as shown after the words e.g. below.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# macro apply duplex ?
 WORD <1-32> Keyword to replace with value e.g. $DUPLEX, $SPEED
 <cr>
switchxxxxxx(config-if)# macro apply duplex $DUPLEX ?
 WORD<1-32> First parameter value
 <cr>
switchxxxxxx(config-if)# macro apply duplex $DUPLEX full $SPEED ? WORD<1-32>
Second parameter value
switchxxxxxx(config-if)# macro apply duplex $DUPLEX full $SPEED 100
```

31.2. macro

Use the `macro` apply/trace Interface Configuration command to either: Apply a macro to an interface without displaying the actions being performed Apply a macro to the interface while displaying the actions being performed

Syntax

- macro {apply | trace} macro-name [parameter-name1 value] [parameter-name2 value] [parameter-name3 value]

Parameters

- apply - Apply a macro to the specific interface.
- trace - Apply and trace a macro to the specific interface.
- macro-name - Name of the macro.
- parameter-name value - For each parameter defined in the macro, specify its name and value. You can enter up to three parameter-value pairs. Parameter keyword matching is case sensitive. All matching occurrences of the parameter name in the macro are replaced with the corresponding value.

Default Configuration

The command has no default setting.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The macro apply command hides the commands of the macro from the user while it is being run. The macro trace command displays the commands along with any errors which are generated by them as they are executed. This is used to debug the macro and find Syntaxor configuration errors.

When you run a macro, if a line in it fails because of a Syntax or configuration error, the macro continues to apply the remaining commands to the interface.

If you apply a macro that contains parameters in its commands, the command fails if you do not provide the values for the parameters. You can use the `macro apply`.

macro-name with a '?' to display the help string for the macro keywords (if you have defined these with the #macro keywords preprocessor command).

Parameter (keyword) matching is case sensitive. All matching occurrences of the parameter are replaced with the provided value. Any full match of a keyword, even if it is part of a large string, is considered a match and replaced by the corresponding value.

When you apply a macro to an interface, the switch automatically generates a macro description command with the macro name. As a result, the macro name is appended to the macro history of the interface. The show parser macro command displays the macro history of an interface.

A macro applied to an interface range behaves the same way as a macro applied to a single interface. When a macro is applied to an interface range, it is applied sequentially to each interface within the range. If a macro command fails on one interface, it is nonetheless attempted to be applied and may fail or succeed on the remaining interfaces.

Examples

Example 1 - The following is an example of a macro being applied to an interface with the trace option.

```
switchxxxxxx(config)# interface te1/0/2
switchxxxxxx(config-if)# macro trace dup $DUPLEX full $SPEED 100
 Applying command… ‘duplex full’ Applying command… ‘speed 100’
switchxxxxxx(config-if)#
```

Example 2 - The following is an example of a macro being applied without the trace option.

```
switchxxxxxx(config)# interface te1/0/2
switchxxxxxx(config-if)# macro apply dup $DUPLEX full $SPEED 100
switchxxxxxx(config-if)#
```

Example 3 - The following is an example of an incorrect macro being applied.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# macro trace dup
```

Applying command...'duplex full'

```
Applying command...'speed auto' % bad parameter value
switchxxxxxx(config-if)#
```

31.3. macro description

Use the `macro description` Interface Configuration mode command to append a description, for example, a macro name, to the macro history of an interface. Use the no form of this command to clear the macro history of an interface. When the macro is applied to an interface, the switch automatically generates a macro description command with the macro name. As a result, the name of the macro is appended to the macro history of the interface.

Syntax

- macro description text
- no macro description

Parameters

- text - Description text. The text can contain up to 160 characters. The text must be double quoted if it contains multiple words.

Default Configuration

The command has no default setting.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

When multiple macros are applied on a single interface, the description text is a concatenation of texts from a number of previously-applied macros.

To verify the settings created by this command, run the `show parser macro` command.

Example

```
switchxxxxxx(config)# interface te1/0/2
switchxxxxxx(config-if)# macro apply dup
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# interface te1/0/3
switchxxxxxx(config-if)# macro apply duplex $DUPLEX full $SPEED 100
switchxxxxxx(config-if)# macro description dup
switchxxxxxx(config-if)# macro description duplex
switchxxxxxx(config-if)# end
switchxxxxxx(config)# exit
switchxxxxxx# show parser macro description
Global Macro(s):
Interface Macro Description(s)
------------ --------------------------------------------------
te1/0/2 dup te1/0/3 duplex | dup | duplex
-----------------------------------------------------------------
switchxxxxxx# configure
switchxxxxxx(config)# interface te1/0/2
switchxxxxxx(config-if)# no macro description
switchxxxxxx(config-if)# end
switchxxxxxx(config)# exit
switchxxxxxx# show parser macro description
Global Macro(s):
Interface Macro Description(s)
--------- --------------------------------------------------
te1/0/3 duplex | dup | duplex
-----------------------------------------------------------------
```

31.4. macro global

Use the `macro global` Global Configuration command to apply a macro to a switch (with or without the trace option).

Syntax

- macro global {apply | trace} macro-name [parameter-name1 value] [parameter-name2 value] [parameter -name3 value]

Parameters

- apply - Apply a macro to the switch.
- trace - Apply and trace a macro to the switch.
- macro-name - Specify the name of the macro.

- parameter-name value - Specify the parameter values required for the switch. You can enter up to three parameter-value pairs. Parameter keyword matching is case sensitive. All matching occurrences of the parameters are replaced with the corresponding value.

Default Configuration

The command has no default setting.

Command Mode

Global Configuration mode

User Guidelines

If a command fails because of a Syntax error or a configuration error when you apply a macro, the macro continues to apply the remaining commands to the switch.

Keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value. Any full match of a keyword, even if it is part of a large string, is considered a match and replaced by the corresponding value.

If you apply a macro that contains keywords in its commands, the command fails if you do not specify the proper values for the keywords when you apply the macro. You can use this command with a '?' to display the help string for the macro keywords. You define the keywords in the help string using the preprocessor command #macro keywords when you define a macro.

When you apply a macro in Global Configuration mode, the switch automatically generates a global macro description command with the macro name. As a result, the macro name is appended to the global macro history. Use `show parser macro` to display the global macro history.

Example.

The following is an example of a macro being defined and then applied to the switch with the trace option.

```
switchxxxxxx(config)# macro name console-timeout
Enter macro commands one per line. End with the character '@'. line console
exec-timeout $timeout-interval
@
switchxxxxxx(config)# macro global trace console-timeout $timeout-interval 100
 Applying command… 'line console'
 Applying command… 'exec-timeout 100'
```

31.5. macro global description

Use the `macro global description` Global Configuration command to enter a description which is used to indicate which macros have been applied to the switch. Use the no form of this command to remove the description.

Syntax

- macro global description text
- no macro global description

Parameters

- text - Description text. The text can contain up to 160 characters.

Default Configuration

The command has no default setting.

Command Mode

Global Configuration mode

User Guidelines

When multiple global macros are applied to a switch, the global description text is a concatenation of texts from a number of previously applied macros.

You can verify your settings by entering the `show parser macro` command with the description keyword.

Examples

```
switchxxxxxx(config)# macro global description "set console timeout interval"
```

31.6. show parser macro

Use the `show parser macro` User EXEC mode command to display the parameters for all configured macros or for one macro on the switch.

Syntax

- show parser macro [{brief | description [interface interface-id | detailed] | name macro-name}]

Parameters

- brief - Display the name of all macros.
- description [interface interface-id] - Display the macro descriptions for all interfaces or if an interface is specified, display the macro descriptions for that interface.
- name macro-name - Display information about a single macro identified by the macro name.
- detailed - Displays information for non-present ports in addition to present ports.

Default Configuration

Display description of all macros on present ports.

If the detailed keyword is not used, only present ports are displayed.

Command Mode

User EXEC mode

Examples

Example 1 - This is a partial output example from the show parser macro command.

```
switchxxxxxx# show parser macro
Total number of macros = 6
--------------------------------------------------------------
Macro name : company-global
Macro type : default global
# Enable dynamic port error recovery for link state
# failures
--------------------------------------------------------------
Macro name : company-desktop
Macro type : default interface
```

```
# macro keywords $AVID
# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1 switchport access
vlan $AVID switchport mode access
```

Example 2 - This is an example of output from the show parser macro name command.

```
switchxxxxxx# show parser macro standard-switch10
Macro name : standard-switch10 Macro type : customizable macro description
standard-switch10 # Trust QoS settings on VOIP packets auto qos voip trust
# Allow port channels to be automatically formed channel-protocol pagp
```

Example 3 - This is an example of output from the show parser macro brief command.

```
switchxxxxxx# show parser macro brief default global : company-global
default interface: company-desktop default interface: company-phone default
interface: company-switch default interface: company-router customizable : snmp
```

Example 4 - This is an example of output from the show parser macro description command.

```
switchxxxxxx# show parser macro description
Global Macro(s): company-global
```

Example 5 - This is an example of output from the show parser macro description interface command.

```
switchxxxxxx# show parser macro description interface te1/0/2
Interface Macro Description
---------------------------------------------------------------
te1/0/2 this is test macro
---------------------------------------------------------------
```

32. Management ACL Commands

32.1. deny (Management)

To set permit rules (ACEs) for the management access list (ACL), use the `deny` Management Access-list Configuration mode command.

Syntax

- deny [interface-id] [service service]
- deny ip-source {ipv4-address | ipv6-address/ipv6-prefix-length} [mask {mask | prefix-length}] [interface-id] [service service]

Parameters

- interface-id - (Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN
- service service - (Optional) Specifies the service type. Possible values are: Telnet, SSH, HTTP, HTTPS and SNMP.
- ipv4-address - Specifies the source IPv4 address.
- ipv6-address/ipv6-prefix-length - Specifies the source IPv6 address and source IPv6 address prefix length. The prefix length must be preceded by a forward slash (/). The parameter is optional.
- mask mask - Specifies the source IPv4 address network mask. The parameter is relevant only to IPv4 addresses.
- mask prefix-length - Specifies the number of bits that comprise the source IPv4 address prefix. The prefix length must be preceded by a forward slash (/). The parameter is relevant only to IPv4 addresses. (Range: 0–32)

Default Configuration

No rules are configured.

Command Mode

Management Access-list Configuration mode

User Guidelines

Rules with ethernet, VLAN, and port-channel parameters are valid only if an IP address is defined on the appropriate interface.

Example

The following example denies all ports in the ACL called mlist.

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# deny
```

32.2. permit (Management)

To set permit rules (ACEs) for the management access list (ACL), use the `permit` Management Access-list Configuration mode command.

Syntax

- permit [interface-id] [service service]
- permit ip-source {ipv4-address | ipv6-address/ipv6-prefix-length} [mask {mask | prefix-length}] [interface-id] [service service]

Parameters

- interface-id - (Optional) Specify an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN
- service service - (Optional) Specifies the service type. Possible values are: Telnet, SSH, HTTP, HTTPS and SNMP.
- ipv4-address - Specifies the source IPv4 address.
- ipv6-address/ipv6-prefix-length - Specifies the source IPv6 address and source IPv6 address prefix length. The prefix length must be preceded by a forward slash (/). The parameter is optional.
- mask mask - Specifies the source IPv4 address network mask. This parameter is relevant only to IPv4 addresses.
- mask prefix-length - Specifies the number of bits that comprise the source IPv4 address prefix. The prefix length must be preceded by a forward slash (/). This parameter is relevant only to IPv4 addresses. (Range: 0–32)

Default Configuration

No rules are configured.

Command Mode

Management Access-list Configuration mode

User Guidelines

Rules with Ethernet, VLAN, and port-channel parameters are valid only if an IP address is defined on the appropriate interface.

Example

The following example permits all ports in the ACL called mlist

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# permit
```

32.3. management access-list

To configure a management access list (ACL) and enter the Management Access-list Configuration mode, use the `management access-list` Global Configuration mode command. To delete an ACL, use the no form of this command.

Syntax

- management access-list name
- no management access-list name

Parameters

- name - Specifies the ACL name. (Length: 1–32 characters)

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

Use this command to configure one of up to 128 management access list. This command enters the Management Access-list Configuration mode, where the denied or permitted access conditions are defined with the deny and permit commands.

If no match criteria are defined, the default value is deny.

When re-entering the access-list context, the new rules are entered at the end of the access list.

Use the `management access-class` command to select the active access list.

The active management list cannot be updated or removed.

For IPv6 management traffic that is tunneled in IPv4 packets, the management ACL is applied first on the external IPv4 header (rules with the service field are ignored), and then again on the inner IPv6 header.

Examples

Example 1 - The following example creates a management access list called mlist, configures management te1/0/1 and te1/0/9, and makes the new access list the active list.

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# permit te1/0/1
switchxxxxxx(config-macl)# permit te1/0/9
switchxxxxxx(config-macl)# exit
switchxxxxxx(config)#
```

Example 2 - The following example creates a management access list called 'mlist', configures all interfaces to be management interfaces except te1/0/1 and te1/0/9, and makes the new access list the active list.

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# deny te1/0/1
switchxxxxxx(config-macl)# deny te1/0/9
switchxxxxxx(config-macl)# permit
switchxxxxxx(config-macl)# exit
switchxxxxxx(config)#
```

32.4. management access-class

To restrict management connections by defining the active management access list (ACL), use the `management access-class` Global Configuration mode command. To disable management connection restrictions, use the no form of this command.

Syntax

- management access-class {console-only | name}
- no management access-class

Parameters

- console-only - Specifies that the device can be managed only from the console.
- name - Specifies the ACL name to be used. (Length: 1–32 characters)

Default Configuration

The default configuration is no management connection restrictions.

Command Mode

Global Configuration mode

Example

The following example defines an access list called mlist as the active management access list.

```
switchxxxxxx(config)# management access-class mlist
```

32.5. show management access-list

To display management access lists (ACLs), use the `show management access-list` Privileged EXEC mode command.

Syntax

- show management access-list [name]

Parameters

- name - (Optional) Specifies the name of a management access list to be displayed. (Length: 1–32 characters)

Default Configuration

All management ACLs are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays the mlist management ACL.

```
switchxxxxxx# show management access-list mlist m1 -deny service telnet permit
te1/0/1 service telnet
! (Note: all other access implicitly denied)
console(config-macl)#
```

32.6. show management access-class

To display information about the active management access list (ACLs), use the `show management access-class` Privileged EXEC mode command.

Syntax

- show management access-class

Parameters

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

Example

The following example displays the active management ACL information.

```
switchxxxxxx# show management access-class
Management access-class is enabled, using access list mlist
```

33. MLD Commands

33.1. clear ipv6 mld counters

To clear the Multicast Listener Discovery (MLD) interface counters, use the `clear ipv6 mld counters` command in Privileged EXEC mode.

Syntax

- clear ipv6 mld counters [interface-id]

Parameters

- interface-id - (Optional) Interface Identifier.

Command Mode

Privileged EXEC mode

User Guidelines

Use the `clear ipv6 mld counters` command to clear the MLD counters, which keep track of the number of joins and leaves received. If you omit the optional

interface-id argument, the clear ipv6 mld counters command clears the counters on all interfaces.

Example

The following example clears the counters for VLAN 100:

```
switchxxxxxx# clear ipv6 mld counters vlan 100
```

33.2. ipv6 mld last-member-query-count

To configure the Multicast Listener Discovery (MLD) last member query counter, use the `ipv6 mld last-member-query-count` command in Interface Configuration mode. To restore the default value, use the no form of this command.

Syntax

- ipv6 mld last-member-query-count count
- no ipv6 mld last-member-query-count

Parameters

- count - The number of times that group- or group-source-specific queries are sent upon receipt of a message indicating a leave. (Range: 1–7)

Default Configuration

A value of MLD Robustness variable.

Command Mode

Interface Configuration mode

User Guidelines

Use the `ipv6 mld robustness` command to change the MLD last member query counter.

Example

The following example changes a value of the MLD last member query counter to 3:

```
switchxxxxxx(config)# interface vlan 1 ipv6 mld last-member-query-count 3 exit
```

33.3. ipv6 mld last-member-query-interval

To configure the Multicast Listener Discovery (MLD) last member query interval, use the `ipv6 mld last-member-query-interval` command in Interface Configuration mode. To restore the default MLD query interval, use the no form of this command.

Syntax

- ipv6 mld last-member-query-interval milliseconds
- no ipv6 mld last-member-query-interval

Parameters

- milliseconds - Interval, in milliseconds, at which MLD group-specific host query messages are sent on the interface. (Range: 100–25500).

Default Configuration

The default MLD last member query interval is 1000 milliseconds.

Command Mode

Interface Configuration mode

User Guidelines

Use the `ipv6 mld last-member-query-interval` command to configure the MLD last member query interval on an interface.

Example

The following example shows how to increase the MLD last member query interval to 1500 milliseconds:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 mld last-member-query-interval 1500
switchxxxxxx(config-if)# exit
```

33.4. ipv6 mld query-interval

To configure the frequency at which the switch sends Multicast Listener Discovery

(MLD) host-query messages, use the `ipv6 mld query-interval` command in Interface Configuration mode. To return to the default frequency, use the no form of this command.

Syntax

- ipv6 mld query-interval seconds
- no ipv6 mld query-interval

Parameters

- seconds - Frequency, in seconds, at which the switch sends MLD query messages from the interface. The range is from 30 to 18000.

Default Configuration

The default MLD query interval is 125 seconds.

Command Mode

Interface Configuration mode

User Guidelines

Use the `ipv6 mld query-interval` command to configure the frequency at which the MLD querier sends MLD host-query messages from an interface. The MLD querier sends query-host messages to discover which multicast groups have members on the attached networks of the router.

The query interval must be bigger than the maximum query response time.

Example

The following example shows how to increase the frequency at which the MLD querier sends MLD host-query messages to 180 seconds:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 mld query-interval 180
switchxxxxxx(config-if)# exit
```

33.5. ipv6 mld query-max-response-time

To configure the maximum response time advertised in Multicast Listener

Discovery (MLD) queries, use the `ipv6 mld query-max-response-time` command in Interface Configuration mode. To restore the default value, use the no form of this command.

Syntax

- ipv6 mld query-max-response-time seconds
- no ipv6 mld query-max-response-time

Parameters

- seconds - Maximum response time, in seconds, advertised in MLD queries. (Range: 5–20)

Default Configuration

10 seconds.

Command Mode

Interface Configuration mode

User Guidelines

This command controls the period during which the responder can respond to an MLD query message before the router deletes the group.

This command controls how much time the hosts have to answer an MLD query message before the router deletes their group. Configuring a value of fewer than 10 seconds enables the router to prune groups faster.

The maximum query response time must be less than the query interval.

Note. If the hosts do not respond fast enough, they might be pruned inadvertently. Therefore, the hosts must know to respond faster than 10 seconds (or the value you configure).

Example

The following example configures a maximum response time of 8 seconds:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 mld query-max-response-time 8
switchxxxxxx(config-if)# exit
```

33.6. ipv6 mld robustness

To configure the Multicast Listener Discovery (MLD) robustness variable, use the `ipv6 mld robustness` command in Interface Configuration mode. To restore the default value, use the no form of this command.

Syntax

- ipv6 mld robustness count
- no ipv6 mld robustness

Parameters

- count - The number of expected packet loss on a link. Parameter range. (Range: 1–7).

Default Configuration

The default value is 2.

Command Mode

Interface Configuration mode

User Guidelines

Use the `ipv6 mld robustness` command to change the MLD robustness variable.

Example

The following example changes a value of the MLD robustness variable to 3:

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 mld robustness 3
switchxxxxxx(config-if)# exit
```

33.7. ipv6 mld version

To configure which version of Multicast Listener Discovery Protocol (MLD) the router uses, use the `ipv6 mld version` command in Interface Configuration mode.

To restore the default value, use the no form of this command.

Syntax

- ipv6 mld version {1 | 2}
- no ipv6 mld version

Parameters

- 1 - MLD Version 1.
- 2 - MLD Version 2.

Default Configuration

1

Command Mode

Interface Configuration mode

User Guidelines

Use the command to change the default version of MLD.

Example

The following example configures the router to use MLD Version 1:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 mld version 1
switchxxxxxx(config-if)# exit
```

33.8. show ipv6 mld counters

To display the Multicast Listener Discovery (MLD) traffic counters, use the `show ipv6 mld counters` command in User EXEC mode.

Syntax

- show ipv6 mld counters [interface-id]

Parameters

- interface-id - (Optional) Interface Identifier.

Command Mode

User EXEC mode

User Guidelines

Use the `show ipv6 mld counters` command to check if the expected number of MLD protocol messages have been received and sent.

If you omit the optional interface-id argument, the show ipv6 mld counters command displays counters of all interfaces.

Example

The following example displays the MLD protocol messages received and sent:

```
switchxxxxxx# show ipv6 mld counters vlan 100
VLAN 100
 Elapsed time since counters cleared:00:00:21
 Failed received Joins: 0
 Total MLDv1 received messages: 10
 Total MLDv2 received messages: 0
 Total invalid received messages: 0
 General Sent Queries: 0
 Specific Sent Queries: 0
```

33.9. show ipv6 mld groups

To display the multicast groups that are directly connected to the router and that were learned through Multicast Listener Discovery (MLD), use the `show ipv6 mld groups` command in User EXEC mode.

Syntax

- show ipv6 mld groups [link-local | group-name | group-address | interface-id] [detail]

Parameters

- link-local - (Optional) Displays the link-local groups.
- group-name | group-address - (Optional) IPv6 address or name of the multicast group.
- interface-id - (Optional) Interface identifier.
- detail - (Optional) Displays detailed information about individual sources.

Command Mode

User EXEC mode

User Guidelines

Use the show ipv6 mld groups [detail] command to display all directly connected groups.

Use the show ipv6 mld groups link-local [detail] command to display all directly connected link-local groups.

Use the show ipv6 mld groups [group-name | group-address] [detail] command to display one given directly connected group.

Use the show ipv6 mld groups interface-id [detail] command to display all groups directly connected to the given interface.

Examples

Example 1. The following is sample output from the show ipv6 mld groups command. It shows all of the groups joined by VLAN 100:

```
switchxxxxxx# show ipv6 mld groups vlan 100
MLD Connected Group Membership
Expires: never - switch itself has joined the group
Group Address  Interface Expires
FF02::2  VLAN 100 never
FF02::1:FF00:1  VLAN 00:10:27
FF02::1:FFAF:2C39  VLAN 100 00:09:11 FF06:7777::1  VLAN 100 00:00:26
```

Example 2. The following is sample output from the show ipv6 mld groups command using the detail keyword:

```
switchxxxxxx# show ipv6 mld groups detail
Expires: zero value - INCLUDE state; non-zero value - EXCLUDE state
Interface: VLAN 100
 Group: FF33::1:1:1
 Router mode: INCLUDE
 Last reporter: 2009:5::12:1 Group Timer Expires: 00:20:11
 Group source list:
 Source Address  Expires
 2004:4::6  00:00:11
 2004:4::16  00:08:11
 Group: FF33::1:1:2
 Router mode: EXCLUDE
 Last reporter: 2008:5::2A:10
 Group Timer Expires: 00:20:11
 Exclude Mode Expiry (Filter) Timer: 00:10:11 Group source list:
 Source Address  Expires
 2004:5::1  00:04:08
 2004:3::1  00:04:08
 2004:7::10  00:00:00
```

```
 2004:50::1  00:00:00
```

33.10. show ipv6 mld groups summary

To display the number of (*, G) and (S, G) membership reports present in the Multicast Listener Discovery (MLD) cache, use the `show ipv6 mld groups summary` command in User EXEC mode.

Syntax

- show ipv6 mld groups summary

Parameters

This command has no arguments or keywords.

Command Mode

User EXEC mode

User Guidelines

The show ipv6 mld groups summary command displays the number of directly connected multicast groups (including link-local groups).

Example

The following is sample output from the show ipv6 mld groups summary command:

switchxxxxxx# show ipv6 mld groups summary

```
MLD Route Summary
 No. of (*,G) routes = 5
 No. of (S,G) routes = 0 Field Descriptions:
No. of (*,G) routes = 5 - Displays the number of groups present in the MLD
cache.
No. of (S,G) routes = 0 - Displays the number of include and exclude mode
sources present in the MLD cache.
```

33.11. show ipv6 mld interface

To display multicast-related information about an interface, use the `show ipv6 mld interface` command in User EXEC mode.

Syntax

- show ipv6 mld interface [interface-id]

Parameters

- interface-id - Interface identifier.

Command Mode

User EXEC mode

User Guidelines

If you omit the optional interface-id argument, the show ipv6 mld interface command displays information about all interfaces.

Example

The following is sample output from the show ipv6 mld interface command for Ethernet interface 2/1/1:

```
switchxxxxxx# show ipv6 mld interface vlan 100
VLAN 100 is up
 Administrative MLD Querier IPv6 address is FE80::260:3EFF:FE86:5649
 Operational MLD Querier IPv6 address is FE80::260:3EFF:FE86:5649
 Current MLD version is 3
 Administrative MLD robustness variable is 2 seconds
 Operational MLD robustness variable is 2 seconds Administrative MLD query
interval is 125 seconds
 Operational MLD query interval is 125 seconds
 Administrative MLD max query response time is 10 seconds
 Operational MLD max query response time is 10 seconds
 Administrative Last member query response interval is 1000 milliseconds
 Operational Last member query response interval is 1000 milliseconds
```

34. MLD Proxy Commands

34.1. ipv6 mld-proxy

To add downstream interfaces to a MLD proxy tree, use the `ip mld-proxy` command in Interface Configuration mode. To remove downstream from interfaces to a MLD proxy tree, use the no form of this command.

Syntax

- ipv6 mld-proxy upstream-interface-id
- no ipv6 mld-proxy

Parameters

- upstream-interface-id - Upstream Interface identifier.

Default Configuration

The protocol is disabled on the interface.

Command Mode

Interface Configuration mode

User Guidelines

Use the `ipv6 mld-proxy` command to add a downstream interface to a MLD proxy tree. If the proxy tree does not exist it is created.

Use the no format of the command to remove the downstream interface. When the last downstream interface is removed from the proxy tree it is deleted too.

Examples

Example 1. The following example adds a downstream interface to a MLD Proxy process with vlan 200 as its Upstream interface:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 mld-proxy vlan 200
switchxxxxxx(config-if)# exit
```

Example 2. The following example adds a range of downstream interfaces to an IGMP Proxy process with vlan 200 as its Upstream interface:

```
switchxxxxxx(config)# interface range vlan 100-105
switchxxxxxx(config-if)# ipv6 mld-proxy vlan 200
switchxxxxxx(config-if)# exit
```

34.2. ipv6 mld-proxy downstream protected

To disable forwarding of IPv6 Multicast traffic from downstream interfaces, use the `ipv6 mld-proxy downstream protected` command in Global Configuration mode. To allow forwarding from downstream interfaces, use the no form of this command.

Syntax

- ipv6 mld-proxy downstream protected
- no ipv6 mld-proxy downstream protected

Parameters

This command has no arguments or keywords.

Default Configuration

Forwarding from downstream interfaces is allowed.

Command Mode

Global Configuration mode

User Guidelines

Use the `ipv6 mld-proxy downstream protected` command to block forwarding from downstream interfaces.

Example

The following example prohibits forwarding from downstream interfaces:

```
switchxxxxxx(config)# ipv6 mld-proxy downstream protected
```

34.3. ipv6 mld-proxy downstream protected interface

To disable or enable forwarding of IPv6 Multicast traffic from a given downstream interface, use the `ipv6 mld-proxy downstream protected interface` command in Interface Configuration mode. To return to default, use the no form of this command.

Syntax

- ipv6 mld-proxy downstream protected interface {enabled | disabled}
- no ipv6 mld-proxy downstream protected interface

Parameters

- enabled - Downstream interface protection on the interface is enabled. IPv6 Multicast traffic arriving on the interface will not be forwarded.
- disabled - Downstream interface protection on the interface is disabled.

IPv6 Multicast traffic arriving on the interface will be forwarded.

Default Configuration

Global downstream protection configuration (see the ipv6 mld-proxy downstream protected command)

Command Mode

Interface Configuration mode

User Guidelines

Use the `ipv6 mld-proxy downstream protected interface disabled` command to block forwarding from the given downstream interface.

Use the `ipv6 mld-proxy downstream protected interface enabled` command to allow forwarding from the given downstream interface.

The command can be configured only for a downstream interface. When a downstream interface is removed from the MLD Proxy tree the configuration is removed too.

Example

The following example prohibits forwarding from downstream interface vlan 100:

```
switchxxxxxx(config)# interface vlan100
switchxxxxxx(config-if)# ipv6 mld-proxy downstream protected interface enabled
switchxxxxxx(config-if)# exit
```

34.4. ipv6 mld-proxy ssm

To define the Source Specific Multicast (SSM) range of IP Multicast addresses, use the `ipv6 mld-proxy ssm` command in Global Configuration mode. To disable the SSM range, use the no form of this command.

Syntax

- ipv6 mld-proxy ssm {default | range access-list}
- no ipv6 mld-proxy ssm

Parameters

- default - Defines the SSM range access list to FF3x::/32 (see rfc4607).
- range access-list - Specifies the standard IPv6 access list name defining the SSM range.

Default Configuration

The command is disabled.

Command Mode

Global Configuration mode

User Guidelines

A new ipv6 mld-proxyssm command overrides the previous ipv6 mld-proxy ssm command.

Use the no ipv6 mld-proxy ssm command to remove all defined ranges.

Example

The following example shows how to configure SSM service for the default IPv6 address range and the IPv6 address ranges defined by access lists list1:

```
switchxxxxxx(config)# ipv6 access-list list1 permit FF7E:1220:2001:DB8::/64
switchxxxxxx(config)# ipv6 access-list list1 deny FF7E:1220:2001:DB1::1
switchxxxxxx(config)# ipv6 access-list list1 permit FF7E:1220:2001:DB1::/64
switchxxxxxx(config)# ipv6 pim mld-proxy range list1
```

34.5. show ipv6 mld-proxy interface

To display information about interfaces configured for MLD Proxy, use the `show ipv6 mld-proxy interface` command in User EXEC mode or Privileged EXEC mode.

Syntax

- show ipv6 mld-proxy interface [interface-id]

Parameters

- interface-id - (Optional) Display MLD Proxy information about the interface.

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

The show ipv6 mld-proxy interface command is used to display all interfaces where the MLD Proxy is enabled or to display the MLD Proxy configuration for a given interface.

Examples

Example 1. The following example displays MLD Proxy status on all interfaces where the MLD Proxy is enabled:

```
switchxxxxxx# show ip mld-proxy interface
* - the switch is the Querier on the interface
IPv6 Forwarding is enabled
IPv6 Multicast Routing is enabled
MLD Proxy is enabled
Global Downdtream interfaces protection is disabled
SSM Access List Name: list1
Interface Type Dicarding IPv6 Multicast vlan 100 upstream
*vlan 102 downstream enabled *vlan 110 downstream default vlan 113 downstream
disabled
```

Example 2. The following is sample output from the show ipv6 mld-proxy interface command for given upstream interface:

```
switchxxxxxx# show ipv6 mld-proxy interface vlan 100
* - the switch is the Querier on the interface
IPv6 Forwarding is enabled
IPv6 Multicast Routing is enabled
MLD Proxy is enabled
Global Downdtream interfaces protection is disabled SSM Access List Name:
vlan 100 is a Upstream interface Downstream interfaces:
 *vlan 102, *vlan 110, vlan 113
```

Example 3. The following is sample output from the show ipv6 mld-proxy interface command for given downstream interface:

```
switchxxxxxx# show ipv6 mld-proxy interface vlan 102
IPv6 Forwarding is enabled
IPv6 Multicast Routing is enabled
MLD Proxy is enabled
Global Downdtream interfaces protection is disabled SSM Access List Name:
default vlan 102 is a Downstream interface
The switch is the Querier on vlan 102
Upstream interface: vlan 100
```

Example 4. The following is sample output from the show ipv6 mld-proxy interface command for an interface on which IGMP Proxy is disabled:

```
switchxxxxxx# show ipv6 mld-proxy interface vlan 1
IPv6 Forwarding is enabled
IPv6 Multicast Routing is enabled
MLD Proxy is disabled
```

35. MLD Snooping Commands

35.1. ipv6 mld snooping (Global)

To enable IPv6 Multicast Listener Discovery (MLD) snooping, use the `ipv6 mld snooping` command in Global Configuration mode. To return to the default, use the no form of this command.

Syntax

- ipv6 mld snooping
- no ipv6 mld snooping

Parameters

N/A

Default Configuration

IPv6 MLD snooping is disabled.

Command Mode

Global Configuration mode

Example

The following example enables IPv6 MLD snooping.

```
switchxxxxxx(config)# ipv6 mld snooping
```

35.2. ipv6 mld snooping vlan

To enable MLD snooping on a specific VLAN, use the `ipv6 mld snooping vlan` command in Global Configuration mode. To return to the default, use the no form of this command.

Syntax

- ipv6 mld snooping vlan vlan-id
- no ipv6 mld snooping vlan vlan-id

Parameters

- vlan-id - Specifies the VLAN.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

MLD snooping can only be enabled on static VLANs.

MLDv1 and MLDv2 are supported.

To activate MLD snooping, bridge multicast filtering must be enabled by the `bridge multicast filtering` command.

The user guidelines of the `bridge multicast mode` command describe the configuration that can be written into the FDB as a function of the FDB mode, and the MLD version that is used in the network.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 2
```

35.3. ipv6 mld snooping querier

To enable globally the MLD Snooping querier, use the `ipv6 mld snooping querier` command in Global Configuration mode. To disable the MLD Snooping querier globally, use the no form of this command.

Syntax

- ipv6 mld snooping querier
- no ipv6 mld snooping querier

Parameters

N/A

Default Configuration

Enabled

Command Mode

Global Configuration mode

User Guidelines

To run the MLD Snooping querier on a VLAN, you have enable it globally and on the VLAN.

Example

The following example disables the MLD Snooping querier globally:

```
switchxxxxxx(config)# no ipv6 mld snooping querier
```

35.4. ipv6 mld snooping vlan querier

To enable the Internet MLD Snooping querier on a specific VLAN, use the `ipv6 mld snooping vlan querier` command in Global Configuration mode. To return to the default, use the no form of this command.

Syntax

- ipv6 mld snooping vlan vlan-id querier
- no ipv6 mld snooping vlan vlan-id querier

Parameters

- vlan-id - Specifies the VLAN.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

The MLD Snooping querier can be enabled on a VLAN only if MLD Snooping is enabled for that VLAN.

Example

The following example enables the MLD Snooping querier on VLAN 1:

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 querier
```

35.5. ipv6 mld snooping vlan querier election

To enable MLD Querier election mechanism of an MLD Snooping querier on a specific VLAN, use the `ipv6 mld snooping vlan querier election` command in Global Configuration mode. To disable Querier election mechanism, use the no form of this command.

Syntax

- ipv6 mld snooping vlan vlan-id querier election
- no ipv6 mld snooping vlan vlan-id querier election

Parameters

- vlan-id - Specifies the VLAN.

Default Configuration

Enabled

Command Mode

Global Configuration mode

User Guidelines

Use the no form of the ipv6 mld snooping vlan querier election command to disable MLD Querier election mechanism on a VLAN.

If the MLD Querier election mechanism is enabled, the MLD Snooping querier supports the standard MLD Querier election mechanism specified in RFC2710 and RFC3810.

If MLD Querier election mechanism is disabled, MLD Snooping Querier delays sending General Query messages for 60 seconds from the time it was enabled. During this time, if the switch did not receive an IGMP query from another Querier - it starts sending General Query messages. Once the switch acts as a Querier, it will stop sending General Query messages if it detects another Querier on the VLAN. In this case, the switch will resume sending General Query messages if it does hear another Querier for Query Passive interval that equals to

<Robustness>*<Query Interval> + 0.5*<Query Response Interval).

See the ipv6 mld robustness, ipv6 mld query-interval, and ipv6 mld query-max-response-time commands for configurations of these parameters.

It is recommended to disable MLD Querier election mechanism if there is an IPMv6 Multicast router on the VLAN.

Example

The following example disables MLD Snooping Querier election on VLAN 1:

```
switchxxxxxx(config)# no ipv6 mld snooping vlan 1 querier election
```

35.6. ipv6 mld snooping vlan querier version

To configure the IGMP version of an IGMP querier on a specific VLAN, use the `ipv6 mld snooping vlan querier version` command in Global Configuration mode. To return to the default, use the no form of this command.

Syntax

- ipv6 mld snooping vlan vlan-id querier version {1 | 2}
- no ipv6 mld snooping vlan vlan-id querier version

Parameters

- vlan-id - Specifies the VLAN.
- querier version {1 | 2} - Specifies the MLD version.

Default Configuration

MLDv1.

Command Mode

Global Configuration mode

Example

The following example sets the version of the MLD Snooping Querier VLAN 1 to 2:

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 querier version 2
```

35.7. ipv6 mld snooping vlan mrouter

To enable automatic learning of Multicast router ports, use the `ipv6 mld snooping vlan mrouter` command in Global Configuration mode. To remove the configuration, use the no form of this command.

Syntax

- ipv6 mld snooping vlan vlan-id mrouter learn pim-dvmrp
- no ipv6 mld snooping vlan vlan-id mrouter learn pim-dvmrp

Parameters

- vlan-id - Specifies the VLAN.
- pim-dvmrp - Learn Multicast router port by PIM, DVMRP and MLD messages.

Default Configuration

Learning pim-dvmrp is enabled.

Command Mode

Global Configuration mode

User Guidelines

Multicast router ports can be configured statically with the `bridge multicast forward-all` command.

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 mrouter learn pim-dvmrp
```

35.8. ipv6 mld snooping vlan mrouter interface

To define a port that is connected to a Multicast router port, use the `ipv6 mld snooping mrouter interface` command in Global Configuration mode. To return to the default, use the no form of this command.

Syntax

- ipv6 mld snooping vlan vlan-id mrouter interface interface-list
- no ipv6 mld snooping vlan vlan-id mrouter interface interface-list

Parameters

- vlan-id - Specifies the VLAN.
- interface-list - Specifies a list of interfaces. The interfaces can be from one of the following types:
  - Port
  - Port-channel.

Default Configuration

No ports defined

Command Mode

Global Configuration mode

User Guidelines

This command may be used in conjunction with the `bridge multicast forward-all` command, which is used in older versions to statically configure a port as a Multicast router.

A port that is defined as a Multicast router port receives all MLD packets (reports and queries) as well as all Multicast data.

You can execute the command before the VLAN is created and for a range of ports as shown in the example.

Example

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# ipv6 mld snooping vlan 1 mrouter interface te1/0/1-4
```

35.9. ipv6 mld snooping vlan forbidden mrouter

To forbid a port from being defined as a Multicast router port by static configuration or by automatic learning, use the `ipv6 mld snooping vlan forbidden mrouter` command in Global Configuration mode. To return to the default, use the no form of this command.

Syntax

- ipv6 mld snooping vlan vlan-id forbidden mrouter interface interface-list
- no ipv6 mld snooping vlan vlan-id forbidden mrouter interface interface-list

Parameters

- vlan-id - Specifies the VLAN.
- interface-list - Specifies list of interfaces. The interfaces can be of one of the following types:
  - Ethernet port

- Port-channel.

Default Configuration

No forbidden ports by default

Command Mode

Global Configuration mode

User Guidelines

A port that is forbidden to be defined as a Multicast router port (mrouter port) cannot be learned dynamically or assigned statically.

The `bridge multicast forward-all` command was used in older versions to forbid dynamic learning of Multicast router ports.

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 forbidden mrouter interface
te1/0/1
```

35.10. ipv6 mld snooping vlan static

To register a IPv6-layer Multicast address to the bridge table, and to add statically ports to the group, use the `ipv6 mld snooping vlan static` command in Global Configuration mode. To return to the default, use the no form of this command.

Syntax

- ipv6 mld snooping vlan vlan-id static ipv6-address [interface interface-list]
- no ipv6 mld snooping vlan vlan-id static ipv6-address [interface interface-list]

Parameters

- vlan-id - Specifies the VLAN.
- ipv6-address - Specifies the IP multicast address
- interface interface-list - (Optional) Specifies list of interfaces. The interfaces can be from one of the following types: Ethernet port or Port-channel.

Default Configuration

No Multicast addresses are defined.

Command Mode

Global Configuration mode

User Guidelines

Static multicast addresses can only be defined on static VLANs.

You can execute the command before the VLAN is created.

You can register an entry without specifying an interface.

Using the no command without a port-list removes the entry.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 static FF12::3 te1/0/1
```

35.11. ipv6 mld snooping vlan immediate-leave

To enable MLD Snooping Immediate-Leave processing on a VLAN, use the `ipv6 mld snooping vlan immediate-leave` command in Global Configuration mode. To return to the default, use the no form of this command.

Syntax

- ipv6 mld snooping vlan vlan-id immediate-leave
- no ipv6 mld snooping vlan vlan-id immediate-leave

Parameters

- vlan-id - Specifies the VLAN ID value. (Range: 1–4094)

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

When an MLD Leave Group message is received from a host, the system removes the host port from the table entry. After it relays the MLD queries from the Multicast router, it deletes entries periodically if it does not receive any MLD membership reports from the Multicast clients.

MLD snooping Immediate-Leave processing allows the switch to remove an interface that sends a leave message from the forwarding table without first sending out MAC-based general queries to the interface.

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 immediate-leave
```

35.12. show ipv6 mld snooping groups

To display the multicast groups learned by the MLD snooping, use the `show ipv6 mld snooping groups` EXEC mode command in User EXEC mode.

Syntax

- show ipv6 mld snooping groups [vlan vlan-id] [address ipv6-multicast-address] [source ipv6-address]

Parameters

- vlan vlan-id - (Optional) Specifies the VLAN ID.
- address ipv6-multicast-address - (Optional) Specifies the IPv6 multicast address.
- source ipv6-address - (Optional) Specifies the IPv6 source address.

Command Mode

User EXEC mode

Default Configuration

Display information for all VLANs and addresses defined on them.

User Guidelines

To see the full multicast address table (including static addresses), use the `show bridge multicast address-table` command.

The Include list contains the ports which are in a forwarding state for this group according to the snooping database. In general, the Exclude list contains the ports which have issued an explicit Exclude for that specific source in a multicast group.

The Reporters That Are Forbidden Statically list contains the list of ports which have asked to receive a multicast flow but were defined as forbidden for that multicast group in a multicast bridge.

Note: Under certain circumstances, the Exclude list may not contain accurate information; for example, in the case when two Exclude reports were received on the same port for the same group but for different sources, the port will not be in the Exclude list but rather in the Include list

Example

The following example shows the output for show ipv6 mld snooping groups.

```
switchxxxxxx# show ipv6 mld snooping groups
VLAN Group Source Address Include Ports Exclude Comp
 Address  Mode
---- -------- ----------------------- ------------- ------- ------
1 FF12::3 FE80::201:C9FF:FE40:8001 te1/0/1 1
1 FF12::3 FE80::201:C9FF:FE40:8002 te1/0/2 1
19 FF12::8 FE80::201:C9FF:FE40:8003 te1/0/4 2
19 FF12::8 FE80::201:C9FF:FE40:8004 te1/0/1 te1/0/2 2
19 FF12::8 FE80::201:C9FF:FE40:8005 te1/0/10-11 te1/0/3 2
MLD Reporters that are forbidden statically:
VLAN Group Address Source Address Ports
---- ------------- ----------------------- -------
1 FF12::3 FE80::201:C9FF:FE40:8001 te1/0/3
19 FF12::8 FE80::201:C9FF:FE40:8001 te1/0/4
```

35.13. show ipv6 mld snooping interface

To display the IPv6 MLD snooping configuration for a specific VLAN, use the `show ipv6 mld snooping interface` EXEC mode command in User EXEC mode.

Syntax

- show ipv6 mld snooping interface vlan-id

Parameters

- vlan-id - Specifies the VLAN ID.

Default Configuration

Display information for all VLANs.

Command Mode User EXEC mode Example

The following example displays the MLD snooping configuration for VLAN 1000.

```
switchxxxxxx# show ipv6 mld snooping interface 1000
MLD Snooping is globally enabled
MLD Snooping Querier is globally enabled
```

```
VLAN 1000
 MLD Snooping is enabled
 MLD snooping last immediate leave: enable
 Automatic learning of multicast router ports is enabled
 MLD Snooping Querier is enabled MLD Snooping Querier operation state: is
running
 MLD Snooping Querier version: 2
 MLD Snooping Querier election is enabled
 MLD snooping robustness: admin 2 oper 2
 MLD snooping query interval: admin 125 sec oper 125 sec
 MLD snooping query maximum response: admin 10 sec oper 10 sec
 MLD snooping last member query counter: admin 2 oper 2
 MLD snooping last member query interval: admin 1000 msec oper 500 msec Groups
that are in MLD version 1 compatibility mode: FF12::3, FF12::8
```

35.14. show ipv6 mld snooping mrouter

To display information on dynamically learned Multicast router interfaces for all VLANs or for a specific VLAN, use the `show ipv6 mld snooping mrouter` EXEC mode command in User EXEC mode.

Syntax

- show ipv6 mld snooping mrouter [interface vlan-id]

Parameters

- interface vlan-id - (Optional) Specifies the VLAN ID.

Default Configuration

Display information for all VLANs.

Command Mode

User EXEC mode

Example

The following example displays information on dynamically learned Multicast router interfaces for VLAN 1000:

```
switchxxxxxx# show ipv6 mld snooping mrouter interface 1000
VLAN Dynamic Static Forbidden
---- ------- ------ ---------
1000 te1/0/1 te1/0/2 te1/0/3-4
```

36. Open Shortest Path First (OSPF) Commands

36.1. area authentication

To enable area default authentication for an Open Shortest Path First (OSPF) area, use the `area authentication` command in router configuration mode. To remove a default authentication specification of an area from the configuration, use the noform of this command.

Syntax

- area area-id authentication [message-digest]
- no area area-id authentication

Parameters

- area-id - Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address.
- message-digest - Enables Message Digest 5 (MD5) authentication on the area specified by the area-id argument.

Default Configuration

Type 0 authentication (no authentication).

Command Mode

Router RIP Configuration mode

User Guidelines

If the area does not exist when the `area authentication` command is applied it is created.

Specifying default authentication for an area without the message-digest keyword sets the authentication to Type 1 (simple password) as specified in RFC 2328, Appendix D. If this command is not included in the configuration file, authentication of Type 0 (no authentication) is assumed.

Use the `ip ospf authentication` interface command to change the area default authentication.

If you enable authentication, you must configure a key chain name with the `ip ospf authentication key-chain` interface command for an IP interface. If a key chain has not been defined for an IP interface or there is not valid key OSPF packets are not sent on the interface and received IP interface packets are dropped.

To remove the default authentication specification for an area, use the no form of this command.

Note:
To remove the specified area from the software configuration, use the `no area area-id` command (with no other keywords). That is, the `no area area-id` command removes all area options, such as area authentication, area default-cost, area nssa, area range, area stub, and area virtual-link.

Example

The following example mandates default authentication for areas 0 and 10.0.0.0. Authentication keys are also provided:

```
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# area 10.0.0.0 authentication
switchxxxxxx(config-ospf)# area 0 authentication
switchxxxxxx(config-ospf)# network 10.56.0.201 area 10.0.0.0
switchxxxxxx(config-ospf)# network 192.168.251.201 area 0
switchxxxxxx(config-ospf)# exit
switchxxxxxx(config)# interface ip 192.168.251.201
switchxxxxxx(config-ip)# ip ospf authentication key-chain chain1
switchxxxxxx(config-ip)# exit
switchxxxxxx(config)# interface ip 10.56.0.201
switchxxxxxx(config-ip)# ip ospf authentication key-chain chain2
switchxxxxxx(config-ip)# exit
```

36.2. area default-cost

To specify a cost for the default summary route that is sent into a stub area or not-so-stubby area (NSSA), use the `area default-cost` command in router address family topology or router configuration mode. To return to default, use the no form of this command.

Syntax

- area area-id default-cost cost
- no area area-id default-cost

Parameters

- area-id - Identifier for the stub area or NSSA. The identifier can be specified as either a decimal value or an IP address.
- Cost - Cost for the default summary route used for a stub or NSSA. The acceptable value is a 24-bit number.

Default Configuration

The default value for area default-cost is 1.

Command Mode

Router RIP Configuration mode

User Guidelines

If the area does not exist when the `area default-cost` command is applied it is created.

This command is used only on an Area Border Router (ABR) attached to a stub area or NSSA. If the area is not a stub area or NSSA or the Router is not an ABR attached to the stub area or NSSA then the configuration is saved but is not applied.

There are two stub area router configuration commands: the `area stub` and `area default-cost` commands. In all routers attached to the stub area, the area should be configured as a stub area using the `area stub` command. The `area default-cost` command impacts only on an ABR attached to the stub area. If the `area default-cost` command is configured on non ABR attached to the area the configuration is saved but it is not applied. The `area default-cost` command provides the metric for the summary default route generated by the ABR into the stub area.

Note:
To remove the specified area from the software configuration, use the `no area area-id` command (with no other keywords). That is, the `no area area-id` command removes all

area options, such as area authentication, area default-cost, area nssa, area range, area stub, and area virtual-link.

Example

The following example assigns a default cost of 20 to stub network 10.0.0.0:

```
switchxxxxxx(config)# interface vlan1
switchxxxxxx(config-if)# ip address 10.56.0.201 255.255.0.0
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# network 10.56.0.201 area 10.0.0.0
switchxxxxxx(config-ospf)# area 10.0.0.0 stub
switchxxxxxx(config-ospf)# area 10.0.0.0 default-cost 20
switchxxxxxx(config-ospf)# exit
```

36.3. area nssa

To configure a not-so-stubby area (NSSA), use the `area nssa` command in router configuration mode. To remove the NSSA distinction from the area, use the no form of this command.

Syntax

- area area-id nssa [no-summary] [translator-role {always | candidate}] [translator-stability-interval seconds]
- no area area-id nssa

Parameters

- area-id - Identifier for the stub area or NSSA. The identifier can be specified as either a decimal value or an IP address.
- no-summary - Allows an area to be an NSSA but not have summary routes injected into it.
- translator-role - Specifies whether or not an NSSA border router will unconditionally translate Type-7 LSAs into Type-5 LSAs. The default value is candidate.
  - Always - Specifies that an NSSA border router always translates Type-7 LSAs into Type-5 LSAs regardless of the translator state of other NSSA border routers.
  - Candidate - Specifies that an NSSA border router participates in the translator election process described in RFC 3101, Section 3.1.
- Seconds - Specifies the number of seconds after an elected translator determines its services are no longer required, that it should continue to perform its translation duties. The default value is 40 seconds.

Default Configuration

No NSSA area is defined.

Command Mode

Router RIP Configuration mode

User Guidelines

If the area does not exist when the `area nssa` command is applied it is created.

The no format of the `area nssa` command does not remove the area, it only changes the area type to transit.

To remove the specified area from the software configuration, use the `no area area-id` command (with no other keywords). That is, the `no area area-id` command removes all area options, including area authentication, area default-cost, area nssa, area range, area stub, and area virtual-link.

Example

The following example makes area 1 an NSSA area:

```
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# redistribute rip subnets
switchxxxxxx(config-ospf)# network 172.19.92.1 area 1
switchxxxxxx(config-ospf)# area 1 nssa
switchxxxxxx(config-ospf)# exit
```

36.4. area range

To consolidate and summarize routes at an area boundary, use the `area range` command in router address family topology or router configuration mode. To disable this function, use the no form of this command.

Syntax

- area area-id range ip-address ip-address-mask [advertise | not-advertise]
- no area area-id range ip-address ip-address-mask

Parameters

- area-id - Identifier of the area for which routes are to be summarized. It can be specified as either a decimal value or an IP address.
- ip-address - IP address.
- ip-address-mask - IP address mask.
- advertise - Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA). If the advertise and non-advertise keywords are omitted the advertise keyword is assumed.
- not-advertise - Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.

Default Configuration

This command is disabled by default.

Command Mode

Router RIP Configuration mode

User Guidelines

If the area does not exist when the `area range` command is configured it is created.

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 range` router configuration commands can be configured. Thus, OSPF can summarize addresses for many different sets of address ranges.

Note:
To remove the specified area from the software configuration, use the `no area area-id` command (with no other keywords). That is, the `no area area-id` command removes all area options, including area authentication, area default-cost, area nssa, area range, area stub, and area virtual-link.

Example

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 36.0.0.0 and for all hosts on network 192.42.110.0:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ip address 192.42.110.201 255.255.255.0
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# interface vlan102
switchxxxxxx(config-if)# ip address 36.56.1.1 255.255.0.0
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# router ospf 201
switchxxxxxx(config-ospf)# network 192.42.110.201 area 0
switchxxxxxx(config-ospf)# network 36.56.1.1 area 36.0.0.0
switchxxxxxx(config-ospf)# area 36.0.0.0 range 10.0.0.0 255.0.0.0
switchxxxxxx(config-ospf)# area 0 range 192.42.110.0 255.255.255.0
switchxxxxxx(config-ospf)# exit
```

36.5. area shutdown

To initiate a graceful shutdown of the Open Shortest Path First (OSPF) protocol in the current area, use the `area shutdown` command in router configuration mode. To restart the OSPF protocol, use the no form of this command.

Syntax

- area area-id shutdown
- no area area-id shutdown

Parameters

- area-id - Identifier for the area. The identifier can be specified as either a decimal value or an IP address.

Default Configuration

OSPF stays active in the current area.

Command Mode

Router RIP Configuration mode

User Guidelines

Use the `area shutdown` command in router configuration mode to temporarily shut down a protocol in the least disruptive manner and to notify its neighbors that it is going away. All traffic that has another path through the network will be directed to that alternate path.

Example

The following example shows how to enable a graceful shutdown of the OSPF protocol in area 10.0.0.0:

```
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# area 10.0.0.0 shutdown
```

```
switchxxxxxx(config-ospf)# exit
```

36.6. area stub

To define an area as a stub area, use the `area stub` command in router address family topology or router configuration mode. To disable this function, use the no form of this command.

Syntax

- area area-id stub [no-summary]
- no area area-id area area-id stub

Parameters

- area-id - Identifier for the stub area. The identifier can be specified as either a decimal value or an IP address.
- no-summary - Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.

Default Configuration

No stub area is defined.

Command Mode

Router RIP Configuration mode

User Guidelines

If the area does not exist when the `area stub` command is configured it is created.

The no format of the `area stub` command does not remove the area, it only changes the area type to transit.

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 route sent into a stub area by an ABR.

There are two `stub area` router configuration commands:

The `area stub` and `area default-cost` commands. In all routers attached to the stub area, the area should be configured as a stub area using the `area stub` command. The `area default-cost` command is needed only on an ABR attached to the stub area. If the `area default-cost` command is configured on non ABR attached to the area the configuration is saved but is not effected. The `area default-cost` command 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. The no-summary keyword configured on non ABR is saved but is not effected.

Note:
To remove the specified area from the software configuration, use the `no area area-id` command (with no other keywords). That is, the `no area area-id` command removes all area options, such as area authentication, area default-cost, area nssa, area range, area stub, and area virtual-link.

Example

The following example assigns a default cost of 20 to stub network 10.0.0.0:

```
switchxxxxxx(config)# router ospf
switchxxxxxx(config-ospf)# network 10.1.1.1 area 10.0.0.0
switchxxxxxx(config-ospf)# area 10.0.0.0 default-cost 20
switchxxxxxx(config-ospf)# area 10.0.0.0 stub
switchxxxxxx(config-ospf)# exit
```

36.7. area virtual-link

To define an Open Shortest Path First (OSPF) virtual link, use the `area virtual-link` command in router address family topology or router configuration mode. To remove a virtual link, use the no form of this command.

Syntax

- area area-id virtual-link router-id [hello-interval seconds] [retransmit-interval seconds] [transmit-delay seconds] [dead-interval seconds] [message-digest | null][key-chain name-of-chain]
- no area area-id virtual-link router-id

Parameters

- area-id - Area ID assigned to the virtual link. This can be either a decimal value or a valid IPv4 prefix. There is no default.
- router-id - Router ID associated with the virtual link neighbor. The router ID appears in the show ip ospf or show ipv6 display command. There is no default.
- hello-interval seconds - Specifies the time (in seconds) between the hello packets that are sent on an interface. The hello interval is an unsigned integer value to be advertised in the hello packets. The value must be the same for all routers and access servers attached to a common network. Range is from 1 to 8192. The default is 10.
- retransmit-interval seconds - Specifies the time (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. The retransmit interval is the expected round-trip delay between any two routers on the attached network. The value must be greater than the expected round-trip delay. Range is from 1 to 8192. The default is 5.
- transmit-delay seconds - Specifies the estimated time (in seconds) required to send a link-state update packet on the interface. The integer value that must be greater than zero. LSAs in the update packet have their age incremented by this amount before transmission. Range is from 1 to 8192. The default value is 1.
- dead-interval seconds - Specifies the time (in seconds) that hello packets are not seen before a neighbor declares the router down. The dead interval is an unsigned integer value. The default is four times the hello interval, or 40 seconds. As with the hello interval, this value must be the same for all routers and access servers attached to a common network.
- message-digest - Specifies that MD5 authentication will be used.
- Null - No authentication is used. Useful for overriding password or message-digest authentication if configured for an area.
- name-of-chain - Specifies the name of key chain.

Default Configuration

No OSPF virtual link is defined.

Command Mode

Router RIP Configuration mode

User Guidelines

In OSPF, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link.

The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. The setting of the retransmit interval should be conservative, or needless retransmissions will result. The value should be larger for serial lines and virtual links.

The transmit delay value should take into account the transmission and propagation delays for the interface.

Note:
In order for a virtual link to be properly configured, each virtual link neighbor must include the transit area ID and the corresponding virtual link neighbor router ID. To see the router ID, use the `show ip ospf` or the `show ipv6 ospf` command in privileged EXEC mode.

Note:
To remove the specified area from the software configuration, use the `no area area-id` command (with no other keywords). That is, the `no area area-id` command removes all area options, including area authentication, area default-cost, area nssa, area range, area stub, and area virtual-link.

Example

Example 1: The following example establishes a virtual link using by a few commands:

```
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# area 1 virtual-link 192.168.255.1
switchxxxxxx(config-ospf)# area 1 virtual-link 192.168.255.1 hello-interval 100
switchxxxxxx(config-ospf)# area 1 virtual-link 192.168.255.1 message-digest key-
chain chain1
switchxxxxxx(config-ospf)# exit
```

Example 2: The following example establishes a virtual link using bone command:

```
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# area 1 virtual-link 192.168.255.1 hello-interval 100
message-digest key-chain chain1
switchxxxxxx(config-ospf)# exit
```

36.8. clear ip ospf process

To restart the Open Shortest Path First (OSPF) process, use the `clear ip ospf process` command in privileged EXEC mode.

Syntax

- clear ip ospf [process-id] process

Parameters

- process-id - Process ID. If the parameter is omitted all the OSPF processes are restarted.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

Use the process-id argument to restart only one OSPF process. If the process-id argument is not specified, all OSPF processes are restarted.

The `clear ip ospf process` command changes the OSPF process router-id if it was reconfigured by the user else if the current used router-id has the default value the command runs the router-id re-election algorithm.

Example

Example 1: The following example restarts all the OSP processes:

```
switchxxxxxx# clear ip ospf process
```

Example 2. The following example restarts one OSP process with process-id 1:

```
switchxxxxxx# clear ip ospf 1 process
```

36.9. compatible rfc1583

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.

Syntax

- compatible rfc1583
- no compatible rfc1583

Parameters

N/A

Default Configuration

Compatible with RFC 1583.

Command Mode

Router RIP Configuration mode

User Guidelines

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.

Example

The following example specifies that the router process is compatible with RFC 1583:

```
switchxxxxxx(config)# router ospf 1
```

```
switchxxxxxx(config-ospf)# compatible rfc1583
switchxxxxxx(config-ospf)# exit
```

36.10. default-information originate (OSPF)

To generate a default external route into an Open Shortest Path First (OSPF) routing domain, use the `default-information originate` command in router configuration or router address family topology configuration mode. To disable this feature, use the no form of this command.

Syntax

- default-information originate [always] [metric metric-value] [metric-type type-value]
- no default-information originate

Parameters

- always - Always advertises the default route regardless of whether the software has a default route.

  Note:
  The always keyword includes the following exception when the route map is used. When a route map is used, the origination of the default route by OSPF is not bound to the existence of a default route in the routing table and the always keyword is ignored.
- metric-value - 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.
- type-value - External link type associated with the default route that is advertised into the OSPF routing domain. It can be one of the following values:
  - Type 1 external route
  - Type 2 external route (default)

Default Configuration

This command is disabled by default. No default external route is generated into the OSPF routing domain.

Command Mode

Router RIP Configuration mode

User Guidelines

Whenever you use the `redistribute` or the `default-information router configuration` command to redistribute routes into an OSPF routing domain, the router becomes an Autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a default route into the OSPF routing domain. The software still must have a default route for itself before it generates one, except when you have specified the always keyword.

When a route map is used, the origination of the default route by OSPF is not bound to the existence of a default route in the routing table.

Example

The following example specifies a metric of 100 for the default route that is redistributed into the OSPF routing domain and an external metric type of Type 1:

```
switchxxxxxx(config)# router ospf 109
switchxxxxxx(config-ospf)# default-information originate metric 100 metric-type
1
switchxxxxxx(config-ospf)# exit
```

36.11. default-metric (OSPF)

To set default metric values for the Open Shortest Path First (OSPF) routing protocol, use the `default-metric` command in router address family topology or router configuration mode. To return to the default state, use the no form of this command.

Syntax

- default-metric metric-value
- no default-metric

Parameters

- metric-value - Default metric value. The range is from 1 to 4294967295.

Default Configuration

Default metric value appropriate for the specified routing protocol.

Command Mode

Router RIP Configuration mode

User Guidelines

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.

Note:
When enabled, the `default-metric` command applies a metric value of 0 to redistributed connected routes. The `default-metric` command does not override metric values that are applied with the `redistribute` command.

Example

The following example specifies a default metric of 100 for that will used for destributed routes from RIP:

`switchxxxxxx(config)#` router ospf 1

```
switchxxxxxx(config-ospf)# default-metric 100
switchxxxxxx(config-ospf)# redistribute rip
switchxxxxxx(config-ospf)# exit
```

36.12. ip ospf authentication

To override the area default authentication type for an IP interface, use the `ip ospf authentication` command in IP interface configuration mode. To return to the area default authentication type for an interface, use the no form of this command.

Syntax

- ip ospf authentication [message-digest | null]
- no ip ospf authentication

Parameters

- message-digest - Specifies that MD5 authentication will be used.
- Null - No authentication is used. Useful for overriding password or message-digest authentication if configured for an area.

Default Configuration

The area default authentication type.

Command Mode

IP Configuration mode

User Guidelines

Specifying default authentication for an area without keyword sets the authentication to Type 1 (simple password) as specified in RFC 2328, Appendix D. If this command is not included in the configuration file, the area default authentication of type is assumed.

If you enable the MD5 authentication, you must configure a key chain name with the `ip ospf authentication key-chain interface` command. If a key chain is not defined for the IP interface or there is not a valid key then RIP packets are not sent on the IP interface and received IP interface packets are dropped.

If you enable the simple password authentication, you must configure a password with the `ip ospf authentication-key interface` command. If a password is not defined for the IP interface then OSPF packets are not sent on the IP interface and received IP interface packets are dropped.

Example

The following example overides the area default authentication for the 10.56.0.201and 10.10.1.1 IP interfaces:

```
switchxxxxxx(config)# router ospf
switchxxxxxx(config-ospf)# area 10.0.0.0 authentication
switchxxxxxx(config-ospf)# network 10.56.0.201 area 10.0.0.0
switchxxxxxx(config-ospf)# network 10.10.1.1 area 10.0.0.0
switchxxxxxx(config-ospf)# network 10.2.1.1 area 10.0.0.0
switchxxxxxx(config-ospf)# exit
switchxxxxxx(config)# interface ip 10.56.0.201
switchxxxxxx(config-ip)# ip ospf authentication message-digest
switchxxxxxx(config-ip)# ip ospf authentication key-chain chain2
switchxxxxxx(config-ip)# exit
switchxxxxxx(config)# interface ip 10.10.1.1
switchxxxxxx(config-ip)# ip ospf authentication null
switchxxxxxx(config-ip)# exit
switchxxxxxx(config)# interface ip 10.2.1.1
switchxxxxxx(config-ip)# ip ospf authentication-key Ases12@@@#$4
switchxxxxxx(config-ip)# exit
```

36.13. ip ospf authentication key-chain

To define a name of key chain to be used by authentication, use the `ip ospf authentication key-chain` command in IP interface configuration mode. To return to default, use the no form of this command.

Syntax

- ip ospf authentication key-chain name-of-chain
- no ip ospf authentication key-chain

Parameters

- name-of-chain - Specifies the name of key chain.

Default Configuration

No key chain is specified.

Command Mode

IP Configuration mode

User Guidelines

Use the `ip ospf authentication key-chain` IP Interface Configuration mode command to define a key chain name. Only one key chaine may be defined per an IP interface. Each `ip ospf authentication key-chain` command overides the previous definition.

Example

The following example defines chain1 and chain2:

```
switchxxxxxx(config)# router ospf
switchxxxxxx(config-ospf)# area 10.0.0.0 authentication
switchxxxxxx(config-ospf)# area 0 authentication
switchxxxxxx(config-ospf)# network 10.56.0.201 area 10.0.0.0
switchxxxxxx(config-ospf)# network 192.168.251.201 area 0
switchxxxxxx(config-ospf)# exit
switchxxxxxx(config)# interface ip 192.168.251.201
switchxxxxxx(config-ip)# ip ospf authentication key-chain chain1
switchxxxxxx(config-ip)# exit
switchxxxxxx(config)# interface ip 10.56.0.201
switchxxxxxx(config-ip)# ip ospf authentication key-chain chain2
switchxxxxxx(config-ip)# exit
```

36.14. ip ospf authentication-key

To assign a password to be used by neighboring routers that are using the OSPF simple password authentication, use the `ip ospf authentication-key` command in IP interface configuration mode. To remove a previously assigned OSPF password, use the no form of this command.

Syntax

- ip ospf authentication-key password
- no ip ospf authentication-key

Parameters

- password - Any continuous string of characters that can be entered from the keyboard up to 8 bytes in length.

Default Configuration

No password is specified.

Command Mode

IP Configuration mode

User Guidelines

The password created by this command is used as a "key" that is inserted directly into the OSPF header when the switch software originates routing protocol packets. A separate password can be assigned to each subnetwork. All neighboring routers on the same subnetwork must have the same password to be able to exchange OSPF information.

Only one password may be defined per an IP interface. Each `ip ospf authentication-key` command overides the previous definition.

Example

The following example shows how to define a password:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip ospf authentication mode text
switchxxxxxx(config-ip)# ip ospf authentication-key alpha$$1267
switchxxxxxx(config-ip)# exit
```

36.15. ip ospf cost

To explicitly specify the cost of sending a packet on an interface, use the `ip ospf cost` command in IP interface configuration mode. To reset the path cost to the default value, use the no form of this command.

Syntax

- ip ospf cost interface-cost
- no ip ospf cost

Parameters

- interface-cost - Unsigned integer value expressed as the link-state metric. It can be a value in the range from 1 to 65535.

Default Configuration

The default value depends on the interface's ifSpeed (see User Guidelines).

Command Mode

IP Configuration mode

User Guidelines

You must define OSPF on an IP interface by the `network` command before using of the `ip ospf cost` command on the same IP interface.

You can set the metric manually using this command, if you need to change the default.

In general, the path cost is calculated using the formula $C_P = 10^{10}$ / ifSpeed.

Using this formula, the default path costs were calculated as noted in the following list. If these values do not suit your network, you can use your own method of calculating path costs.

- 10G Ethernet Default cost is 1
- 1G Ethernet Default cost is 10
- 100M Ethernet Default cost is 100
- 10M Ethernet Default cost is 1000

Example

The following example sets the interface cost value to 65:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip ospf cost 65
switchxxxxxx(config-ip)# exit
```

36.16. ip ospf dead-interval

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 IP interface configuration mode. To restore the default value, use the no form of this command.

Syntax

- ip ospf dead-interval seconds
- no ip ospf dead-interval

Parameters

- seconds - Interval (in seconds) during which the router must receive at least one hello packet from a neighbor or else that neighbor is removed from the peer list and does not participate in routing. The range is 1 to 65535. The value must be the same for all nodes on the network.

Default Configuration

Four times the interval set by the `ip ospf hello-interval` command.

Command Mode

IP Configuration mode

User Guidelines

The dead interval is advertised in OSPF hello packets. This value must be the same for all networking devices on a specific network.

Example

The following example sets the OSPF dead interval to 20 seconds:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip ospf dead-interval 20
switchxxxxxx(config-ip)# exit
```

36.17. ip ospf hello-interval

To specify the interval between hello packets that are sent on the IP interface, use the `ip ospf hello-interval` command in IP interface configuration mode. To return to the default time, use the no form of this command.

Syntax

- ip ospf hello-interval seconds

- no ip ospf hello-interval

Parameters

- seconds - Specifies the interval (in seconds). The value must be the same for all nodes on a specific network. The range is from 1 to 65535.

Default Configuration

10 seconds

Command Mode

IP Configuration mode

User Guidelines

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.

Example

The following example sets the interval between hello packets to 15 seconds:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip ospf hello-interval 15
switchxxxxxx(config-ip)# exit
```

36.18. ip ospf mtu-ignore

To disable Open Shortest Path First (OSPF) maximum transmission unit (MTU) mismatch detection on receiving Database Descriptor (DBD) packets, use the `ip ospf mtu-ignore` command in IP interface configuration mode. To reset to default, use the no form of this command.

Syntax

- ip ospf mtu-ignore
- no ip ospf mtu-ignore

Parameters

N/A

Default Configuration

OSPF MTU mismatch detection is enabled.

Command Mode

IP Configuration mode

User Guidelines

OSPF 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, OSPF adjacency will not be established.

Example

The following example disables MTU mismatch detection on receiving DBD packets:

```
switchxxxxxx(config)# interface ip 1.1.1.1
```

```
switchxxxxxx(config-ip)# ip ospf mtu-ignore
switchxxxxxx(config-ip)# exit
```

36.19. ip ospf name-lookup

To configure Open Shortest Path First (OSPF) to look up Domain Name System (DNS) names for use in all OSPF show EXEC command displays, use the `ip ospf name-lookup` command in global configuration mode. To disable this function, use the no form of this command.

Syntax

- ip ospf name-lookup
- no ip ospf name-lookup

Parameters

N/A

Default Configuration

This command is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

This command makes it easier to identify a router because the router is displayed by name rather than by its router ID or neighbor ID.

Example

The following example configures OSPF to look up DNS names for use in all OSPF show EXEC command displays:

```
switchxxxxxx(config)# ip ospf name-lookup
```

36.20. ip ospf passive-interface

To disable sending OSPF routing updates on an IP interface, use the `ip ospf passive-interface` command in IP interface configuration mode. To re-enable the sending of OSPF routing updates, use the no form of this command.

Syntax

- ip ospf passive-interface
- no ip ospf passive-interface

Parameters

N/A

Default Configuration

Routing updates are sent on the interface.

Command Mode

IP Configuration mode

User Guidelines

OSPF routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the OSPF domain.

Example

The following example sets all OSPF IP interfaces as passive and then activates Ethernet interface 0:

```
switchxxxxxx(config)# router ospf 100
switchxxxxxx(config-ospf)# network 1.1.1.1 area 0
switchxxxxxx(config-ospf)# passive-interface default
switchxxxxxx(config-ospf)# exit
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# no passive-interface
switchxxxxxx(config-ip)# exit
```

36.21. ip ospf priority

To set the router priority, which helps determine the designated router for this network, use the `ip ospf priority` command in IP interface configuration mode. To return to the default value, use the no form of this command.

Syntax

- ip ospf priority number-value
- no ip ospf priority

Parameters

- number-value - A number value that specifies the priority of the router. The range is from 0 to 255.

Default Configuration

Priority of 1.

Command Mode

IP Configuration mode

User Guidelines

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 multiaccess networks (in other words, not to point-to-point networks).

Example

The following example sets the router priority value to 4:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip ospf priority 4
switchxxxxxx(config-ip)# exit
```

36.22. ip ospf retransmit-interval

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the IP interface, use the `ip ospf retransmit-interval` command in IP interface configuration mode. To return to the default value, use the no form of this command.

Syntax

- ip ospf retransmit-interval seconds
- no ip ospf retransmit-interval

Parameters

- seconds - Time (in seconds) between retransmissions. The range is from 1 to 65535 seconds. The default is 5 seconds.

Default Configuration

5 seconds.

Command Mode

IP Configuration mode

User Guidelines

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 the *seconds* argument should be greater than the expected round-trip delay between any two routers on the attached network. The setting of this parameter should also be conservative, or needless LSA retransmissions may occur. The value should be larger for serial lines and virtual links.

Note:
It is recommended to use the same value for the seconds argument on neighbor OSPF routers. Using inconsistent values on neighbor routers can cause needless LSA retransmissions.

Example

The following example sets the retransmit interval value to 8 seconds:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip ospf retransmit-interval 8
switchxxxxxx(config-ip)# exit
```

36.23. ip ospf shutdown

To initiate an Open Shortest Path First (OSPF) protocol graceful shutdown at the IP interface level, use the `ip ospf shutdown` command in interface configuration mode. To restart the OSPF protocol on an interface, use the no form of this command.

Syntax

ip ospf shutdown no ip ospf shutdown

Parameters

N/A

Default Configuration

N/A

Command Mode

IP Configuration mode

User Guidelines

Use the `ip ospf shutdown` command to put OSPF on a specific interface in shutdown mode.

Example

The following example shows how to initiate an OSPF protocol shutdown on IP interface 1.1.1.1:

```
switchxxxxxx(config)# interface ip 1.1.1
switchxxxxxx(config-ip)# ip ospf shutdown
switchxxxxxx(config-ip)# exit
```

36.24. ip ospf transmit-delay

To set the estimated time required to send a link-state update packet on the IP interface, use the `ip ospf transmit-delay` command in IP interface configuration mode. To return to the default value, use the no form of this command.

Syntax

- ip ospf transmit-delay seconds
- no ip ospf transmit-delay

Parameters

- seconds - Time (in seconds) required to send a link-state update. The range is from 1 to 65535 seconds. The default is 1 second.

Default Configuration

1 second.

Command Mode

IP Configuration mode

User Guidelines

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.

Example

The following example sets the retransmit delay value to 3 seconds:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip ospf transmit-delay 3
switchxxxxxx(config-ip)# exit
```

36.25. ip ospf ttl-security

To configure the Time-to-Live (TTL) security check feature on a specific interface, use the `ip ospf ttl-security` command in interface configuration mode. To disable TTL security on an interface, use the no form of this command.

Syntax

- ip ospf ttl-security [hops hop-count |disable]
- no ip ospf ttl-security

Parameters

- hop-count - Configures the maximum number of IP hops. The hop-count argument range is from 1 to 254.
- Disable - Disables TTL security on an interface.

Default Configuration

TTL security is disabled on all Open Shortest Path First (OSPF) interfaces.

Command Mode

Interface Configuration mode

User Guidelines

Use the `ip ospf ttl-security` command to configure TTL security on a specific interface.

The disable keyword can be used to disable TTL security on a specific interface but is only useful if the `ttl-security all-interfaces` command was used to first configure TTL security on all OSPF interfaces. In this way, all OSPF interfaces can be configured with TTL security and then individual interfaces can be disabled. This can save time as opposed to configuring each interface one-by-one from the start.

Example

The following example shows how to effectively use the disable keyword to disable TTL security on Ethernet interface 0/0 after the feature has first been configured on all OSPF interfaces:

```
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# ttl-security all-interfaces
switchxxxxxx(config-ospf)# exit
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ip ospf ttl-security disable
switchxxxxxx(config-if)# exit
```

36.26. log-adjacency-changes

To configure the router to send a syslog message when an Open Shortest Path First (OSPF) neighbor goes up or down, use the `log-adjacency-changes` command in router configuration mode. To turn off this function, use the no form of this command.

Syntax

- log-adjacency-changes [detail]
- no log-adjacency-changes

Parameters

- detail - Sends a syslog message for each state change, not just when a neighbor goes up or down.

Default Configuration

Enabled

Command Mode

Router RIP Configuration mode

User Guidelines

This command allows you to know about OSPF neighbors going up or down. The `log-adjacency-changes` command provides a high level view of those changes of the peer relationship. The `log-adjacency-changes` command is on by default but only up/down (full/down) events are reported, unless the detail keyword is also used.

Example

The following example configures the router to send a syslog message when an OSPF neighbor state changes:

```
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# log-adjacency-changes default
switchxxxxxx(config-ospf)# exit
```

36.27. network area

To define the IP 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 ip-address wildcard-mask pair, use the no form of this command.

Syntax

- network ip-address area area-id [shutdown]
- no network ip-address

Parameters

- ip-address - IP address.
- area-id - Area that is to be associated with the OSPF address range. It can be specified as either a decimal value or as an IP address. If you intend to associate areas with IP subnets, you can specify a subnet address as the value of the area-id argument.
- Shutdown - OSPF is enabled on the interface in the shutdown state

Default Configuration

This command is disabled by default.

Command Mode

Router RIP Configuration mode

User Guidelines

OSPF can be defined only on manually configured IP interfaces, meaning that RIP cannot be defined on an IP address defined by DHCP or on a default IP address.

Use the `network` CLI command with the shutdown keyword to create OSPF on an interface if you are going to change the default values of RIP configuration and the use the `no ip ospf shutdown` CLI command.

Use the `no network` CLI command to remove OSPF on an IP interface and remove its interface configuration.

Note:
Any individual IP interface can only be attached to a single area. If the address ranges specified for different areas overlap, the software will adopt the first area in the network command list and ignore the subsequent overlapping portions. In general, we recommend that you configure address ranges that do not overlap in order to avoid inadvertent conflicts.

Example

Example 1:The following example shows how to enable OSPF on IP interface 1.1.1.1 with the default interface configuration:

```
switchxxxxxx(config)# router ospf
switchxxxxxx(config-ospf)# network 1.1.1.1 area 0
switchxxxxxx(config-ospf)# exit
```

Example 2: The following example enables OSPF on 1.1.1.1 in the shutdown state, configures the interface cost and starts OSPF:

```
switchxxxxxx(config)# router ospf
switchxxxxxx(config-ospf)# network 1.1.1.1 area 0 shutdown
switchxxxxxx(config-ospf)# exit
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip ospf cost 102
switchxxxxxx(config-ip)# no ip ospf shutdown
switchxxxxxx(config)# exit
```

36.28. no area

To remove the specified area from the software configuration, use the `no area` command in router configuration mode.

Syntax

- no area area-id

Parameters

- area-id - Identifier for the removed area. The identifier can be specified as either a decimal value or an IP address.

Default Configuration

Area is defined.

Command Mode

Router RIP Configuration mode

User Guidelines

To remove the specified area from the software configuration, use the `no area area-id` command. That is, the `no area area-id` command removes all area options, including area authentication, area default-cost, area nssa, area range, area stub, and area virtual-link.

Example

The following example removes area 1:

```
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# no area 1
switchxxxxxx(config-ospf)# exit
```

36.29. passive-interface (OSPF)

To disable sending OSPF routing updates on all OSPF IP interfaces, use the `passive-interface` command in router configuration mode. To re-enable the sending of OSPF routing updates, use the no form of this command.

Syntax

- passive-interface
- no passive-interface

Parameters

N/A

Default Configuration

Routing updates are sent on all OSPF IP interfaces.

Command Mode

Router RIP Configuration mode

User Guidelines

OSPF routing information is neither sent nor received through all OSPF IP interfaces. A passive IP interface address appears as a stub network in the OSPF domain.

After using of the `passive-interface` command you can then configure individual interfaces where adjacencies are desired using the `no ip ospf passive-interface` command. The `passive-interface` command is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

Example

The following example sets all OSPF IP interfaces as passive and then activates IP interface 1.1.1.1:

```
switchxxxxxx(config)# router ospf 100
switchxxxxxx(config-ospf)# network 1.1.1.1 area 0
switchxxxxxx(config-ospf)# passive-interface
switchxxxxxx(config-ospf)# exit
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# no ip ospf passive-interface
switchxxxxxx(config-ip)# exit
```

36.30. redistribute (OSPF)

To redistribute routes from one routing domain into OSPF routing domain, use the `redistribute` command in the appropriate configuration mode. To disable redistribution, use the no form of this command.

Syntax

- redistribute protocol [process-id] [metric metric-value] [metric-type type-value] [match {internal | external 1| external 2}] [subnets] [nssa-only]
- no redistribute protocol [process-id] [metric metric-value] [metric-type type-value] [match {internal | external 1| external 2}] [subnets] [nssa-only]

Parameters

- protocol - Source protocol from which routes are being redistributed. It can be one of the following keywords:
  - connected,
  - static,
  - rip,
  - ospf or
  - bgp.
- process-id - The process-id argument is used only together with the ospf keyword and specifies the appropriate OSPF process ID from which routes are to be redistributed. This identifies the routing process. This value takes the form of a nonzero decimal number. If it is omitted then a value of 1 is assumed.
- metric metric-value - Specifies the metric assigned to the redistributed routes.
  - If the metric value is set by the route map (by the set metric command) then the value will supersede the metric value specified by the metric-value argument.
  - If no metric is specified, the following metric is assigned depending on the source protocol:
  - from OSPF
  - the internal OSPF metric from the redistribution source process is advertised as the external metric in the redistribution destination process.
  - the external OSPF metric from the redistribution source process is advertised as the external metric with value of 1.
  - from BGP – 1
  - from any protocol except OSPF and BGP - 20
- metric-type type-value - Specifies the external link type associated with the default route advertised into the OSPF routing domain. It can be one of two values:
  - 1 - Type 1 external route
  - 2 - Type 2 external route
  - If a metric-type is not specified, a Type 2 external route is adopted.
- match {internal | external 1 | external 2} - The match keyword is used only together with the ospf keyword and specifies the criteria by which OSPF routes are redistributed into the target OSPF process. It can be one of the following:
  - internal - Routes that are internal to a specific autonomous system.
  - external 1 - Routes that are external to the autonomous system, but are imported into OSPF as Type 1 external route.
  - external 2 - Routes that are external to the autonomous system, but are imported into OSPF as Type 2 external route.
  - By default the internal and external 1 routes are redistributed.
    Note:
    A few the redistribute commands with different values of the match keyword may be defined.

- Subnets - For redistributing routes into OSPF, the scope of redistribution for the specified protocol. If the subnets keyword is not specified, only routes that are not subnetted are redistributed. By default, no subnets are defined.
- nssa-only - Sets the nssa-only attribute for all routes redistributed into OSPF. On a router internal to an NSSA area, the nssa-only keyword causes the originated type-7 NSSA LSAs to have their propagate (P) bit set to zero, which prevents area border routers from translating these LSAs into type-5 external LSAs. On an area border router that is connected to a NSSA and normal areas, the nssa-only keyword causes the routes to be redistributed only into the NSSA areas.

Default Configuration

Route redistribution is disabled.

Command Mode

Router RIP Configuration mode

User Guidelines

Routes distributed to the source protocol are never redistributed by it.

The connected keyword is used to redistribute to the target OSPF autonomous system routes that correspond to defined IP interfaces on which the destination OSPF process is not enabled. By default, the OSPF process advertises only IP interfaces on which the OSPF process is enabled.

The static keyword is used to redistribute to the target OSPF process static routes. By default, static routes are not redistributed to OSPF.

Changing or disabling any keyword will not affect the state of other keywords.

A router receiving a link-state protocol with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric only considers the advertised metric to reach the destination.

Whenever you use the `redistribute` or the default-information router configuration commands to redistribute routes into an OSPF routing domain, the router automatically becomes an ASBR. However, an ASBR does not, by default, generate a default route into the OSPF routing domain.

Removing options that you have configured for the redistribute command requires careful use of the no form of the redistribute command to ensure that you obtain the result that you are expecting.

Example

Example 1: The following example causes RIP routes to be redistributed into an OSPF domain:

```
switchxxxxxx(config)# router ospf 110
switchxxxxxx(config-ospf)# redistribute rip metric 200 subnets
switchxxxxxx(config-ospf)# exit
```

Example 2: In the following example, network 172.16.0.0 will appear as an external link-state advertisement (LSA) in OSPF 1 with a cost of 100 (the cost is preserved):

```
switchxxxxxx(config)# interface vlan 2 0
switchxxxxxx(config-if)# ip address 172.16.0.1 255.0.0.0
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# interface vlan 10
switchxxxxxx(config-if)# ip address 10.0.0.1 255.0.0.0
```

```
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# router ospf 2
switchxxxxxx(config-ospf)# network 172.16.0.1 area 0
switchxxxxxx(config-ospf)# exit
switchxxxxxx(config)# interface ip 172.16.0.1
switchxxxxxx(config-ip)# ip ospf cost 100
switchxxxxxx(config-ip)# exit
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# network 10.0.0.1 area 0
switchxxxxxx(config-ospf)# redistribute ospf 2 subnet
switchxxxxxx(config-ospf)# exit
```

Example 3: In the following example, internal route are redistributed from OSPF process 1 to OSPF process 2 with their metrics as external 1; external 1 routes are redistributed with metric equal to 100 as external 1 and external 2 routes are redistributed with metric equal to 200 as external 2 :

```
switchxxxxxx(config)# router ospf 2
switchxxxxxx(config-ospf)# redistribute ospf 1 match internal metric-type 1 subnet
switchxxxxxx(config-ospf)# redistribute ospf 1 match external 1 metric-type 1 metric
100 subnet
switchxxxxxx(config-ospf)# redistribute ospf 1 match external 2 metric-type 2 metric
200 subnet
switchxxxxxx(config-ospf)# exit
```

Example 4: The following example removes the subnets options:

```
switchxxxxxx(config)# router ospf 2
switchxxxxxx(config-ospf)# no redistribute ospf subnets
switchxxxxxx(config-ospf)# exit
```

36.31. router ospf

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.

Syntax

- router ospf [process-id]
- no router ospf [process-id]

Parameters

- 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. The default value is 1.

Default Configuration

No OSPF routing process is defined.

Command Mode

Global Configuration mode

User Guidelines

The no format of the `router ospf` command removes the OSPF configuration.

Use the `TBD` command to disable OSPF without OSPF configuration removing.

Example

The following example configures an OSPF routing process:

```
switchxxxxxx(config)# router ospf 2
```

36.32. router-id

To use a fixed router ID, use the `router-id` command in router configuration mode. To return to the default, use the no form of this command.

Syntax

- router-id ip-address
- no router-id ip-address

Parameters

- ip-address - Router ID in IP address format.

Default Configuration

The minimum IPv4 address configured on the router.

Command Mode

Router RIP Configuration mode

User Guidelines

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 process` command.

Example

The following example specifies a fixed router-id:

```
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# router-id 10.1.1.1
switchxxxxxx(config-ospf)# exit
```

36.33. show ip ospf

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.

Syntax

- show ip ospf [process-id]

Parameters

- process-id - Process ID. If this argument is included, only information for the specified routing process is included.

Command Mode

User EXEC mode

Privileged EXEC mode

Example

The following is sample output from the `show ip ospf` command:

```
switchxxxxxx# show ip ospf
OSPF Routing Process 1 with ID 192.168.0.0
  Administrative state is UP
  Default Redistribute Metric is 100
  Redistributing is enabled from
    Connected:
      metric value is default metric
      metric type is external 2
      with subnets
      nssa only
    Connected:
      metric value is default metric
      metric type is external 2
      with subnets
      nssa only
    static:
      metric value is 50
      metric type is external 1
      without subnets
    OSPF 109:
      internal:
        internal metric value is preserved, metric type is external 1
          metric value is preserved, metric type is external 1
           with subnets
        external 1
          metric value is 100, metric type is external 1
           with subnets
        external 2
          metric is value 100, metric type is external 2
           with subnets
    OSPF 120:
      from metric type:
        internal: metric value is default metric, metric type is external 1
          metric value is default metric, metric type is external 1
           with subnets
        external 1: metric value is default metric, metric type is external 2
          metric value is default metric, metric type is external 2
           with subnets
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  It is an Autonomous System Boundary Router
  It is an Area Boundary Router
  It is RFC1583 Compatible
  SPF schedule delay 5000 ms
  Maximum Number of Equal Cost Paths 4
  Number of External LSAs (Type 5) is 6, Checksum is 0x11029BEB
  Number of Opaque External LSAs (Type11) is 0, Checksum is 0x0
  Number of originated LSAs is 126
  Number of received LSAs is 1006
    Area BACKBONE(0)
      Administrative state is UP
      Number of interfaces in this area is 2
      Area has message digest authentication
```

```
    SPF algorithm executed 4 times
    Area ranges are
      192.168.0.0/16 Advertise
      192.100.0.0/16 Not Advertise
    Number of ASBR is 0
    Number of ABR is 2
    Number of LSA in this area is 10. Checksum Sum 0x29BEB
    Number of Router LSA(Type 1) 2. Checksum Sum 0x2929BEB
    Number of Network LSA(Type 2) 3. Checksum Sum 0x2929000
    Number of Summary IP Network LSA(Type 3) 3. Checksum Sum 0xBEB
    Number of Summary ASBR LSA(Type 4) 2. Checksum Sum 0x2929BEB
    Number of Opaque Link-Local LSAs (Type 9) is 0, Checksum is 0x0
    Number of Opaque Area-Local LSAs (Type 10) is 0, Checksum is 0x0
  Area 24
    Administrative state is UP
    Number of interfaces in this area is 2
    Area has no authentication
    SPF algorithm executed 10 times
    Area ranges are
    Number of ASBR is 1
    Number of ABR is 3
    Number of Router LSA(Type 1) 2. Checksum Sum 0x2929BEB
    Number of Network LSA(Type 2) 3. Checksum Sum 0x2929000
    Number of Summary IP Network LSA(Type 3) 3. Checksum Sum 0xBEB
    Number of Summary ASBR LSA(Type 4) 2. Checksum Sum 0x2929BEB
    Number of Opaque Link-Local LSAs (Type 9) is 0, Checksum is 0x0
    Number of Opaque Area-Local LSAs (Type 10) is 0, Checksum is 0x0
  Area 10.0.0.0
    It is a NSSA area
    Administrative state is UP
    Number of interfaces in this area is 4
    Area default metric is 100
    Perform type-7/type-5 LSA translation, suppress forwarding address
    Number of Router LSA(Type 1) 2. Checksum Sum 0x2929BEB
    Number of Network LSA(Type 2) 3. Checksum Sum 0x2929000
    Number of Summary IP Network LSA(Type 3) 3. Checksum Sum 0xBEB
    Number of Summary ASBR LSA(Type 4) 2. Checksum Sum 0x2929BEB
    Number of Opaque Link-Local LSAs (Type 9) is 0, Checksum is 0x0
    Number of Opaque Area-Local LSAs (Type 10) is 0, Checksum is 0x0
  Area 192.168.1.1
    It is a stub area, no summary
    Administrative state is UP
    Number of interfaces in this area is 4
    Area default metric is 100
    Number of Router LSA(Type 1) 2. Checksum Sum 0x2929BEB
    Number of Network LSA(Type 2) 3. Checksum Sum 0x2929000
    Number of Summary IP Network LSA(Type 3) 3. Checksum Sum 0xBEB
    Number of Opaque Link-Local LSAs (Type 9) is 0, Checksum is 0x0
    Number of Opaque Area-Local LSAs (Type 10) is 0, Checksum is 0x0
```

36.34. show ip ospf border-routers

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.

Syntax

- show ip ospf border-routers

Command Mode

Privileged EXEC mode

Example

The following is sample output from the show ip ospf border-routers command:

```
switchxxxxxx# show ip ospf border-routers
OSPF Routing Process 4 with ID 10.10.24.4
                  Internal Routing Table
Destination     Route  Route  Next Hop       Outgoing   Router     Route
Router ID       Type   Cost   IP Address     Interface  Type       Area ID
192.168.97.53   Intr   10     172.16.1.53    VLAN 1      ABR       0.0.0.3
192.168.103.51  Intr   10     192.168.96.51  VLAN 2      ABR,      0.0.0.3
192.168.103.52  Inte   22     192.168.96.51  VLAN 3      ASBR      0.0.0.3
192.168.103.52  Inte   22     172.16.1.53    VLAN 100    ASBR,ABR  0.0.0.3
```

Field's descriptions:

- Destination Router ID - Router ID of the destination.
- Route Type
  - Intr - Intra-area route,
  - Inte - Inter-area route.
- Route Cost - Cost of using this route.
- Next Hop IP Address - Next hop toward the destination.
- Outgoing Interface - Outgoing interface toward the destination.
- Router Type - The router type of the destination: it is either an ABR or ASBR or both.
- Route Area ID - The area ID of the area from which this route is learned.

36.35. show ip ospf database

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.

Syntax

- show ip ospf [process-id [area-id]] database show ip ospf [process-id [area-id]] database [adv-router [ip-address]] show ip ospf [process-id [area-id]] database [asbr-summary] [link-state-id]
- show ip ospf [process-id [area-id]] database [asbr-summary] [link-state-id] [adv-router
- [ip-address]] show ip ospf [process-id [area-id]] database [asbr-summary] [link-state-id] [self-originate]
- [link-state-id]
- show ip ospf [process-id [area-id]] database [database-summary] show ip ospf [process-id [area-id]] database [external] [link-state-id] show ip ospf [process-id [area-id]] database [external] [link-state-id] [adv-router [ip-address]] show ip ospf [process-id [area-id]] database [external] [link-state-id] [self-originate] [link-state-id] show ip ospf [process-id [area-id]] database [network] [link-state-id] show ip ospf [process-id [area-id]] database [network] [link-state-id] [adv-router [ip-address]] show ip ospf [process-id [area-id]] database [network] [link-state-id] [self-originate]

[link-state-id] show ip ospf [process-id [area-id]] database [nssa-external] [link-state-id]

- show ip ospf [process-id [area-id]] database [nssa-external] [link-state-id] [adv-router [ip-address]]
- show ip ospf [process-id [area-id]] database [nssa-external] [link-state-id] [self-originate]
- [link-state-id] show ip ospf [process-id [area-id]] database [router] [link-state-id] show ip ospf [process-id [area-id]] database [router] [adv-router [ip-address]] show ip ospf [process-id [area-id]] database [router] [self-originate] [link-state-id] show ip ospf [process-id [area-id]] database [self-originate] [link-state-id] show ip ospf [process-id [area-id]] database [summary] [link-state-id] show ip ospf [process-id [area-id]] database [summary] [link-state-id] [adv-router [ip-address]] show ip ospf [process-id [area-id]] database [summary] [link-state-id] [self-originate] [link-state-id]

Parameters

- process-id - 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.
- area-id - Area number associated with the OSPF address range defined in the network router configuration command used to define the particular area.
- adv-router [ip-address] - 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).
- link-state-id - 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.
  When the link state advertisement is describing a network, the link-state-id can take one of two forms:
  - The network's IP address (as in type 3 summary link advertisements and in autonomous system external link advertisements).
  - A derived address obtained from the link state ID. (Note that masking a network links advertisement's link state ID with the network's subnet mask yields the network's IP address.)

  When the link state advertisement is describing a router, the link state ID is always the described router's OSPF router ID.
  When an autonomous system external advertisement (LS Type = 5) is describing a default route, its link state ID is set to Default Destination (0.0.0.0).
- asbr-summary - Displays information only about the autonomous system boundary router summary LSAs.
- database-summary - Displays how many of each type of LSA for each area there are in the database, and the total.
- External - Displays information only about the external LSAs.
- Network - Displays information only about the network LSAs.
- nssa-external - Displays information only about the NSSA external LSAs.
- Router - Displays information only about the router LSAs.
- self-originate - Displays only self-originated LSAs (from the local router).
- Summary - Displays information only about the summary LSAs.

Command Mode

User EXEC mode

User Guidelines

The various forms of this command deliver information about different OSPF link state advertisements.

Example

Example 1: The following is sample output from the `show ip ospf database` command when no arguments or keywords are used:

```
switchxxxxxx# show ip ospf database
OSPF Routing Process 300 with ID 192.168.239.66
                Displaying Router Link States(Area 0.0.0.0)
Link ID         ADV Router      Age   Seq#         Checksum  Link count
--------------- --------------- ----- ------------ ---------- ---------
172.16.21.6     172.16.21.6     1731  0x80002CFB   0x69BC     8
172.16.21.5     172.16.21.5     1112  0x800009D2   0xA2B8     5
172.16.1.2      172.16.1.2      1662  0x80000A98   0x4CB6     9
172.16.1.1      172.16.1.1      1115  0x800009B6   0x5F2C     1
172.16.1.5      172.16.1.5      1691  0x80002BC    0x2A1A     5
172.16.65.6     172.16.65.6     1395  0x80001947   0xEEE1     4
172.16.241.5    172.16.241.5    1161  0x8000007C   0x7C70     1
172.16.27.6     172.16.27.6     1723  0x80000548   0x8641     4
172.16.70.6     172.16.70.6     1485  0x80000B97   0xEB84     6
                Displaying Net Link States(Area 0.0.0.0)
Link ID         ADV Router        Age   Seq#         Checksum
--------------- ---------------- ----- ------------ ----------
172.16.1.3      192.168.239.66   1245  0x800000EC   0x82E
                Displaying Summary Net Link States(Area 0.0.0.0)
Link ID         ADV Router        Age   Seq#         Checksum
--------------- ---------------- ----- ------------ ----------
172.16.240.0    172.16.241.5     1152  0x80000077   0x7A05
172.16.241.0    172.16.241.5     1152  0x80000070   0xAEB7
172.16.244.0    172.16.241.5     1152  0x80000071   0x95CB
```

Example 2: The following is sample output from the `show ip ospf database` command with the asbr-summary keyword:

```
switchxxxxxx# show ip ospf database asbr-summary
OSPF Routing Process 300 with ID 192.168.239.66
                Displaying Summary ASB Link States(Area 0.0.0.0)
LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links(AS Boundary Router), Type 4
Link State ID: 172.16.245.1 (AS Boundary Router address)
Advertising Router: 172.16.241.5
LS Seq Number: 0x80000072
LS Checksum: 0x3548
LS Length: 28
Network Mask: 0.0.0.0
TOS: 0  Metric: 1
```

Example 3: The following is sample output from the `show ip ospf database` command with the external keyword:

```
switchxxxxxx# show ip ospf database external
OSPF Routing Process 300 with ID 192.168.239.66
                  Displaying AS External Link States
LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link, Type 5
Link State ID: 10.105.0.0 (External Network)
Advertising Router: 172.16.70.6
LS Seq Number: 0x80000AFD
LS Checksum: 0xC3A
LS Length: 36
Network Mask: 255.255.0.0
TOS: 0
  Metric Type: 2 (Larger than any link state path)
  Metric: 1
  Forward Address: 0.0.0.0
  External Route Tag: 0
```

Example 4: The following is sample output from the `show ip ospf database` command with the network keyword:

```
switchxxxxxx# show ip ospf database network
OSPF Routing Process 300 with ID 192.168.239.66
                Displaying Network Link States(Area 0.0.0.0)
LS age: 1367
Options: (No TOS-capability)
LS Type: Network Links, Type 2
Link State ID: 172.16.1.3 (address of Designated Router)
Advertising Router: 192.168.239.66
LS Seq Number: 0x800000E7
LS Checksum: 0x1229
LS Length: 52
Network Mask: 255.255.255.0
  Attached Router: 192.168.239.66
  Attached Router: 172.16.241.5
  Attached Router: 172.16.1.1
  Attached Router: 172.16.54.5
  Attached Router: 172.16.1.5
```

Example 5: The following is sample output from the `show ip ospf database` command with the router keyword:

```
switchxxxxxx# show ip ospf database router
OSPF Routing Process 300 with ID 192.168.239.66
Displaying Router Link States(Area 0.0.0.0)
LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links, Type 1
Link State ID: 172.16.21.6
Advertising Router: 172.16.21.6
LS Seq Number: 0x80002CF6
LS Checksum: 0x73B7
LS Length: 120
AS Boundary Router
Number of Links: 8
  Link connected to: another Router (point-to-point)
```

```
    Link ID) Neighboring Router ID: 172.16.21.5
    (Link Data) Router Interface address: 172.16.21.6
    Number of TOS metrics: 0
    TOS 0  Metrics: 2
  Link connected to: another Router (transit network
    Link ID) Neighboring Router ID: 182.16.21.5
    (Link Data) Designated Router: 182.18.21.6
    Number of TOS metrics: 0
    TOS 0  Metrics: 2
```

Example 6: The following is sample output from `show ip ospf database` command with the summary keyword:

```
switchxxxxxx# show ip ospf database summary
OSPF Routing Process 300 with ID 192.168.239.66
                Displaying Summary Net Link States(Area 0.0.0.0)
LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links(Network), Type 3
Link State ID: 172.16.240.0 (summary Network Number)
Advertising Router: 172.16.241.5
LS Seq Number: 0x80000072
LS Checksum: 0x84FF
LS Length: 28
Network Mask: 255.255.255.0 TOS: 0  Metric: 1
```

Example 7: The following is sample output from `show ip ospf database` command with the database-summary keyword:

```
switchxxxxxx# show ip ospf database database-summary
OSPF Routing Process 1 with ID 10.0.1.1
Area 0 database summary
  LSA Type          Count
  Router            3
  Network           0
  Summary Net       0
  Summary ASBR      0
  Type-7 Ext        0
  Opaque Link       0
  Opaque Area       0
  Subtotal          3

Process 1 database summary

  LSA Type          Count
  Router            2
  Network           0
  Summary Net       2
  Summary ASBR      0
  Type-7 Ext        0
  Opaque Link       0
  Opaque Area       0
  Opaque AS         0
  Total             4
```

Example 8: The following is sample output from the `show ip ospf database` command with the nssa-external keyword:

```
switchxxxxxx# show ip ospf database nssa-external
OSPF Routing Process 300 with ID 192.168.239.66
                  Displaying NSSA External Link States
LS age: 280
Options: (No TOS-capability)
LS Type: NSSA External Link, Type 7
Link State ID: 10.105.0.0 (External Network)
Advertising Router: 172.16.70.6
LS Seq Number: 0x80000AFD
LS Checksum: 0xC3A
LS Length: 36
Network Mask: 255.255.0.0
TOS: 0
  Metric Type: 2 (Larger than any link state path)
  Metric: 1
  Forward Address: 0.0.0.0
  External Route Tag: 0
```

36.36. show ip ospf interface

To display OSPF interface information related to Open Shortest Path First (OSPF), use the `show ip ospf interface` command in user EXEC or privileged EXEC mode.

Syntax

- show ip ospf [process-id] interface [ip-address] [brief]

Parameters

- process-id - Process ID number. If this argument is included, only information for the specified routing process is included. Range is from 1 to 65535.
- ip-address - Interface IP address.
- Brief - Displays brief overview information for OSPF interfaces, states, addresses and masks, and areas on the router.

Command Mode

User EXEC mode

Privileged EXEC mode

Example

Example 1: The following is sample output from the `show ip ospf interface` command when Ethernet interface 0/0 is specified:

```
switchxxxxxx# show ip ospf interface
OSPF Routing Process 1 with ID 192.168.0.0
Internet Address 192.168.254.202/24, Area 0
  Interface VLAN 10, BROADCAST is up, IP Interface is up, OSPF Adminastrative
state is up
  Cost: 10
  IP Interface has message digest authentication, key chain name is chain99
  Transmit Delay is 1 sec
  Priority 1
```

```
  Hello Interval  is 10  sec, Dead Interval is 40 sec, Retransmit Interval is 5
sec
  It is a Designated Router
  Designated Router (ID) 192.168.99.1, Interface address 192.168.254.202
  Backup Designated router (ID) 192.168.254.10, Interface address 192.168.254.10
  Number of LSAs 120, Checksum 0x11029BEB
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.254.10  (Backup Designated Router)
Internet Address 192.168.25.202/24, Area 0
  Interface VLAN 10, BROADCAST is up, IP Interface is up, OSPF Adminastrative
state is is up
  It is  a passive interface
  Cost: 10
  IP Interface has no authentication
  Transmit Delay is 1 sec
  Priority 1
  Hello Interval  is 10  sec, Dead Interval is 40 sec, Retransmit Interval is 5
sec
  Designated Router (ID) 192.168.9.10, Interface address 192.168.25.20
  Backup Designated router (ID) 192.168.25.10, Interface address 192.168.25.10
  Transmit Delay is 1 sec
  Number of LSAs 120, Checksum 0x11029BEB
  Neighbor Count is 3, Adjacent neighbor count is 0
Internet Address 192.168.250.202/24, Area 0
  Interface VLAN 10, BROADCAST is up, IP Interface is up, OSPF on interface is
down
  It is  a passive interface
  Cost: 10
  IP Interface has no authentication
  Transmit Delay is 1 sec
  Priority 1
  Hello Interval  is 10  sec, Dead Interval is 40 sec, Retransmit Interval is 5
sec
Internet Address 192.168.250.202/24, Area 0
  Interface VLAN 10, BROADCAST is up, IP Interface is down, OSPF Adminastrative
state is up   Cost: 10
  IP Interface has no authentication
  Transmit Delay is 1 sec
  Priority 1
  Hello Interval  is 10  sec, Dead Interval is 40 sec, Retransmit Interval is 5
sec
Internet Address 192.168.50.202/24, Area 0
  Interface VLAN 10, BROADCAST is down, IP Interface is down, OSPF
Adminastrative state is up   Cost: 10
  IP Interface has no authentication
  Transmit Delay is 1 sec
  Priority 1
  Hello Interval  is 10  sec, Dead Interval is 40 sec, Retransmit Interval is 5
sec
```

Example 2: The following sample output from `the show ip ospf interface brief` command shows a summary of information:

```
switchxxxxxx# show ip ospf interface brief
IP Interface     Process ID Area ID         Cost Auth Type OSPF Oper St Passive
---------------- ---------- --------------- ---- --------- ------------ -------
```

```
172.116.211.116  1          172.116.211.116 10   digest    up           Yes
1.1.2.1          1          1.1.2.0         35             down
1.1.3.1          1          20              55             up
```

36.37. show ip ospf neighbor

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.

Syntax

- show ip ospf [process-id] neighbor [interface ip-address] [neighbor-id] [detail]

Parameters

- process-id - Process ID number. If this argument is included, only information for the specified routing process is included. Range is from 1 to 65535.
- interface ip-address - Interface IP address.
- neighbor-id - Neighbor hostname or IP address in A.B.C.D format.
- Detail - Displays all neighbors given in detail (lists all neighbors).

Command Mode

Privileged EXEC mode

Example

Example 1: The following is sample output from the `show ip ospf neighbor` command showing a single line of summary information for each neighbor:

```
switchxxxxxx# show ip ospf neighbor
Neighbor Addr    Neighbor ID       PID  IP Interface     Pri State    Dead Time
---------------- ----------------- ---- ---------------- --- -------- ---------
192.199.199.137  100.199.199.137     1  192.199.199.100  100 Exch/OTH  00:00:31
2.1.1.1          1.1.1.1             2  2.2.2.12         100 TwoW/OTH  00:01:31
3.1.1.1          30.1.1.1            3  2.2.2.12         100 ExSt/OTH  00:01:31
4.1.1.12         40.1.1.1            2  4.2.2.12         100 Exch/OTH  00:01:31
5.1.1.1          50.1.1.1            2  5.2.2.12         100 Load/OTH  00:01:31
6.1.1.1          6.1.1.1             2  6.2.2.12         100 Load/BDR  00:01:31
7.1.1.1          7.1.1.1             2  7.2.2.12         100 Load/DR   00:01:31
```

Example 2: The following is sample output showing summary information about the neighbor that matches the neighbor ID:

```
switchxxxxxx# show ip ospf neighbor 10.199.199.137
Neighbor 10.199.199.137, interface address 192.168.80.37
  Process ID 1, Area 0.0.0.0, Interface 10.199.80.1
  Neighbor priority is 1, State is FULL
  Options 2
  Dead timer due in 0:00:32
  Link State retransmission due in 0:00:04
Neighbor 10.199.199.137, interface address 172.16.48.189
  Process ID 1, Area 0.0.0.0, Interface 172.16.50.19
  Neighbor priority is 5, State is FULL
  Options 2
  Dead timer due in 0:00:32
  Link State retransmission due in 0:00:03
```

Example 3: If you specify the interface along with the neighbor ID, the system displays the neighbors that match the neighbor ID on the interface, as in the following sample display:

```
switchxxxxxx# show ip ospf neighbor interface 192.168.80.100 10.199.199.137
Neighbor 10.199.199.137, interface address 192.168.80.37
  Process ID 1, Area 0.0.0.0, Interface 192.168.80.100
  Neighbor priority is 1, State is FULL
  Options 2
  Dead timer due in 0:00:37
  Link State retransmission due in 0:00:04
```

Example 4. You can also specify the interface without the neighbor ID to show all neighbors on the specified interface, as in the following sample display:

```
switchxxxxxx# show ip ospf neighbor interface 172.16.50.1
Neighbor Addr  Neighbor ID      PID  IP Interface  Pri  State     Dead Time
-------------- ---------------- ---- ------------- ---- --------- ---------
172.16.50.2    100.199.199.137  1    172.16.50.1   100  Exch/OTH  00:00:31
172.16.50.3    1.1.1.1          1    172.16.50.1   10   TwoW/OTH  00:01:31
172.16.50.4    30.1.1.1         1    172.16.50.1   120  ExSt/OTH  00:01:31
```

Example 5: The following is sample output from the `show ip ospf neighbor detail` command :

```
switchxxxxxx# show ip ospf neighbor 192.168.5.2 detail
Neighbor 192.168.5.2, interface address 10.225.200.28
  Process ID 1, Area 0.0.0.0, Interface 10.199.80.1
  Neighbor priority is 1, State is FULL, 6 state changes
  DR is 10.225.200.28 BDR is 10.225.200.30
  Options is 0x42
  LLS Options is 0x1 (LR), last OOB-Resync 00:03:08 ago
  Dead timer due in 00:00:36
  Number requested LSAs 0
  Retransmission queue length 0
```

36.38. show ip ospf router-id

To display OSPF process router-id, use the `show ip ospf router-id` command in user EXEC or privileged EXEC mode.

Syntax

- show ipv6 ospf [process-id] router-id

Parameters

- process-id - Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.

Default Configuration

N/A

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

The process-id argument can be entered as a decimal number or as an IPv6 address format.

Example

The following is sample output from the `show ip ospf router-id` command:

```
switchxxxxxx# show ip ospf router-id
Process-ID     Current Router-ID          Next Router-ID after Restart
            Value               Type      Value                Type
----------- ------------------- --------- -------------------- ---------
          1  1.1.1.192           default   1.1.1.1              default
          2  1.1.1.192           default   100.100.100.100      manual
          3  2.2.2.2             manual    2.2.2.2              default
          4  10.10.10.10         manual    1.1.1.1              default
          5  10.10.10.10         manual    2.2.2.2              manual
```

36.39. show ip ospf snmp

To display OSPF snmp configuration, use the `show ip ospf snmp` command in user EXEC or privileged EXEC mode.

Syntax

- show ip ospf snmp

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

Use the `show ipv6 ospf snmp` command to display the OSPF snmp configuration.

Example

The following is sample output from the `show ip ospf snmp` command:

```
switchxxxxxx# show ip ospf snmp
The standard OSPF MIB is mapped to OSPF process 2
SNMP notifications for OSPF are enabled
SNMP notifications Rate Limit: 10 seconds and 7 notifications during the window
time
Authentication Failure Notifications are enabled
Bad Packet Notifications are disabled
Configuration Error Notifications are enabled
Virtual Link Authentication-failure Notifications are disabled
Virtual Link Bad Packet Notifications are enabled
Virtual Link Configuration Error Notifications are enabled
SNMP LSA Notifications are disabled
SNMP Packet Retransmission Notifications are disabled
SNMP Virtual Packet Retransmission Notifications are disabled
SNMP IF State Change Notifications are enabled
SNMP Neighbor State Change Notifications are enabled
SNMP Virtual IF State Change Notifications are enabled
SNMP Virtual Neighbor State Change Notifications are enabled
```

36.40. show ip ospf virtual-links

To display parameters and the current state of Open Shortest Path First (OSPF) virtual links, use `the show ip ospf virtual-links` command in EXEC mode.

Syntax

- show ip ospf virtual-links [process-id]

Parameters

- process-id - Process ID. If this argument is included, only information for the specified routing process is included.

Command Mode

User EXEC mode

User Guidelines

The information displayed by the `show ip ospf virtual-links` command is useful in debugging OSPF routing operations.

Example

The following is sample output from the `show ip ospf virtual-links` command:

```
switchxxxxxx# show ip ospf virtual-links
OSPF Routing Process 4 with ID 10.10.24.4
Virtual Link to router 192.168.101.2,  Transit area 0.0.0.1
  Virtual Link State is UP Virtual Link  Cost is 100
  Virtual Link has message digest authentication, key chain name is chain1
  Hello Interval  is 10  sec, Dead Interval is 40 sec, Retransmit Interval is 5
sec
  Transmit Delay is 1 sec
Virtual Link to router 192.16.10.2, Transit area 10.0.0.1
  Virtual Link State DOWN
  Virtual Link has no authentication
  Hello Interval  is 10  sec, Dead Interval is 40 sec, Retransmit Interval is 5
sec
  Transmit Delay is 1 sec
```

36.41. shutdown (OSPF)

To initiate a graceful shutdown of the Open Shortest Path First (OSPF) protocol under the current instance, use the `shutdown` command in router configuration mode. To restart the OSPF protocol, use the no form of this command.

Syntax

- Shutdown
- no shutdown

Parameters

N/A

Default Configuration

OSPF stays active under the current instance.

Command Mode

Router RIP Configuration mode

User Guidelines

Use the `shutdown` command in router configuration mode to temporarily shut down a protocol in the least disruptive manner and to notify its neighbors that it is going away. All traffic that has another path through the network will be directed to that alternate path.

The `no shutdown` command changes the OSPF process router-id if it was reconfigured by the user else if the current used router-id has the default value the command runs the router-id re-election algorithm.

Example

The following example shows how to enable a graceful shutdown of the OSPF protocol:

```
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# shutdown
switchxxxxxx(config-ospf)# exit
```

36.42. snmp-process ospf

To specify an OSPF process accessed via the standard OSPF MIB, use the `snmp-process ospf` command in global configuration mode. To return to the default, use the no form of this command.

Syntax

- snmp-process ospf process-id
- no snmp-process [process-id]

Parameters

- process-id - OSPF process ID.

Default Configuration

The minimal existed OSPF process.

Command Mode

Global Configuration mode

User Guidelines

The standard MIB do not include the OSPF process-ID and by default is mapped to the minimal OSPF process. Use the `snmp-process` command to change the mapping.

Example

The following example maps the standard MIBs to OSPF process 100:

```
switchxxxxxx(config)# snmp-process ospf 100
```

36.43. snmp-server enable traps ospf

To enable all Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF), use the `snmp-server enable traps ospf` command in global configuration mode. To disable all SNMP notifications for OSPF, use the no form of this command.

Syntax

- snmp-server enable traps ospf
- no snmp-server enable traps ospf

Parameters

N/A

Default Configuration

SNMP notifications for OSPF are disabled.

Command Mode

Global Configuration mode

User Guidelines

If you wish to enable or disable specific OSPF SNMP notifications, enter one or more of the following commands:

```
[no] snmp-server enable traps ospf errors
[no] snmp-server enable traps ospf lsa
[no] snmp-server enable traps ospf retransmit
[no] snmp-server enable traps ospf state-change
```

Example

The following exampleglobally enables SNMP notifications for OSPF:

```
switchxxxxxx(config)# snmp-server enable traps ospf
```

36.44. snmp-server enable traps ospf errors

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) errors, use the `snmp-server enable traps ospf errors` command in global configuration mode. To disable SNMP notifications for OSPF errors, use the no form of this command.

Syntax

- snmp-server enable traps ospf errors [authentication-failure][bad-packet] [config-error] [virt-authentication-failure] [virt-bad-packet] [virt-config-error]
- no snmp-server enable traps ospf errors [authentication-failure][bad-packet] [config-error] [virt-authentication-failure] [virt-bad-packet] [virt-config-error]

Parameters

- authentication-failure - Enables only the ospfIfFailure trap. Allows SNMP notifications to be sent when a packet has been received on a nonvirtual interface from a neighbor router whose authentication key or authentication type conflicts with the authentication key or authentication type of this router.
- bad-packet - Enables only the ospfIfRxBadPacket trap. Allows SNMP notifications to be sent when an OSPF packet that has not been parsed has been received on a nonvirtual interface.
- config-error - Enables only the ospfIfConfigError trap. Sends SNMP notifications when a packet has been received in a nonvirtual interface from a neighbor router whose configuration parameters conflict with the configuration parameters of this router.

- virt-authentication-failure - Enables only the ospfVirtIfFailure trap. Allows SNMP notifications to be sent when a packet has been received on a virtual interface from a neighbor router whose authentication key or authentication type conflicts with the authentication key or authentication type of this router.
- virt-bad-packet - Enables only the ospfVirtIfRxBadPacket trap. Allows SNMP notifications to be sent when an OSPF packet that has not been parsed has been received on a virtual interface.
- virt-config-error - Enables only the ospfVirtIfConfigError trap. Sends SNMP notifications when a packet has been received in a virtual interface from a neighbor router whose configuration parameters conflict with the configuration parameters of this router.

Default Configuration

SNMP notifications for OSPF errors are disabled.

Command Mode

Global Configuration mode

User Guidelines

When you enter the `snmp-server enable traps ospf errors` command without any optional keywords, all OSPF error traps will be enabled. To enable only one or more OSPF error traps, enter one or more of the optional keywords.

Example

The following example enables the router to send all OSPF error notifications:

```
switchxxxxxx(config)# snmp-server enable traps ospf errors
```

36.45. snmp-server enable traps ospf lsa

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) link-state advertisements (LSAs), use the `snmp-server enable traps ospf lsa` command in global configuration mode. To disable SNMP notifications for OSPF LSAs, use the no form of this command.

Syntax

- snmp-server enable traps ospf lsa [lsa-maxage] [lsa-originate]
- no snmp-server enable traps ospf lsa [lsa-maxage] [lsa-originate]

Parameters

- lsa-maxage - Enables the ospfMaxAgeLsa trap
- lsa-originate - Enables the ospfOriginateLsa trap

Default Configuration

SNMP notifications for OSPF LSAs are disabled.

Command Mode

Global Configuration mode

User Guidelines

The `snmp-server enable traps ospf lsa` command enables the traps for standard LSAs that are defined by the OSPF-MIB. To enable the ospfMaxAgeLsa trap, enter the `snmp-server enable traps ospf lsa` command with the lsa-maxage keyword. To enable

the ospfOriginateLsa trap, enter the `snmp-server enable traps ospf lsa` command with the lsa-originate keyword. When the ospfOriginateLsa trap is enabled, it will not be invoked for simple LSA refreshes that take place every 30 minutes or when an LSA has reached its maximum age and is being flushed. When you enter the `snmp-server enable traps ospf lsa` command without either keyword, both traps will be enabled.

Example

The following example enables the router to send SNMP notifications when new LSAs are originated by the router as a result of a topology change:

```
switchxxxxxx(config)# snmp-server enable traps ospf lsa lsa-originate
```

36.46. snmp-server enable traps ospf rate-limit

To limit the number of Open Shortest Path First (OSPF) traps that are sent during a specified number of seconds, use the `snmp-server enable traps ospf rate-limit` command in global configuration mode. To disable the limit placed on the number of OSPF traps sent during a specified number of seconds, use the no form of this command.

Syntax

- snmp-server enable traps ospf rate-limit seconds trap-number
- no snmp-server enable traps ospf rate-limit seconds trap-number

Parameters

- seconds - Sets the rate limit window size, in seconds. A number from 2 to 60. The default value is 10.
- trap-number - Sets the maximum number of traps sent during the window time. A number from 0 to 300. The default number is 7.

Default Configuration

No limit is placed on the number of OSPF traps sent.

Command Mode

Global Configuration mode

User Guidelines

There is a possibility that a router sends trap bursts, which can drain network resources in a small interval of time. It is recommended that you enter the `snmp-server enable traps ospf rate-limit` command to configure a sliding window mechanism that will limit the number of traps that are sent within a specified number of seconds

Example

The following example sets the trap rate limit window so that during a 40-second window of time, no more that 50 traps are sent:

```
switchxxxxxx(config)# snmp-server enable traps ospf rate-limit 40 50
```

36.47. snmp-server enable traps ospf retransmit

To enable Simple Network Management Protocol (SNMP) notifications when packets are re-sent in an Open Shortest Path First (OSPF) network, use the `snmp-server enable traps ospf retransmit` command in global configuration mode. To disable SNMP notifications, use the no form of this command.

Syntax

- snmp-server enable traps ospf retransmit [packets] [virt-packets]
- no snmp-server enable traps ospf retransmit [packets] [virt-packets]

Parameters

- packets - Enables only the ospfTxRetransmit trap. Allows SNMP notifications to be sent when an OSPF packet has been re-sent on a nonvirtual interface.
- virt-packets - Enables only the ospfVirtTxRetransmit trap. Allows SNMP notifications to be sent when an OSPF packet has been re-sent on a virtual interface.

Default Configuration

SNMP notifications are disabled.

Command Mode

Global Configuration mode

User Guidelines

To enable the ospfTXRetransmit trap so that SNMP notifications are sent only when packets from nonvirtual interfaces are re-sent, enter the `snmp-server enable traps ospf retransmit` command with the packets keyword. To enable the ospfTxRetransmit trap so that SNMP notifications are sent only when packets from virtual interfaces are re-sent, enter the `snmp-server enable traps ospf retransmit` command with the virt-packets keyword. When you enter the `snmp-server enable traps ospf retransmit` command without either keyword, both traps will be enabled.

Example

The following example enables the router to send SNMP notifications when packets are re-sent by virtual interfaces:

```
switchxxxxxx(config)# snmp-server enable traps ospf retransmit virt-packets
```

36.48. snmp-server enable traps ospf state-change

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) transition state changes, use the snmp-server enable traps ospf state-change command in global configuration mode. To disable SNMP notifications for OSPF transition state changes, use the no form of this command.

Syntax

- snmp-server enable traps ospf state-change [if-state-change] [neighbor-state-change] [virtif-state-change] [virtneighbor-state-change]
- no snmp-server enable traps ospf state-change [if-state-change] [neighbor-state-change] [virtif-state-change] [virtneighbor-state-change]

Parameters

- if-state-change - Enables only the ospfIfStateChange trap. Sends SNMP notifications when there has been a change in the state of a nonvirtual OSPF interface.
- neighbor-state-change - Enables only the ospfNbrStateChange trap. Sends SNMP notifications when there has been a change in the state of a nonvirtual OSPF neighbor.
- virtif-state-change - Enables only the ospfVirtIfStateChange trap. Sends SNMP notifications when there has been a change in the state of a virtual OSPF interface.

- virtneighbor-state-change - Enables only the ospfVirtNbrStateChange trap. Sends SNMP notifications when there has been a change in the state of a virtual OSPF neighbor.

Default Configuration

SNMP notifications for OSPF transition state changes are disabled.

Command Mode

Global Configuration mode

User Guidelines

To enable all traps for transition state changes, enter the snmp-server enable traps ospf state-change command without of the optional keywords.

Example

The following example enables the router to send SNMP notifications for transition state changes for virtual interfaces and virtual neighbors:

```
switchxxxxxx(config)# snmp-server enable traps ospf state-change virtif-state-change virtneighbor-state-change
```

36.49. summary-address

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.

Syntax

- summary-address {ip-address mask | ip-address/mask-length} [not-advertise] [nssa-only]
- no summary-address summary-address {ip-address mask | ip-address/mask-length} [not-advertise] [nssa-only]

Parameters

- ip-address mask - Summary address range designated for a range of addresses in format ip address and ip mask.
- ip-address/mask-length - Summary address range designated for a range of addresses in forma ip address and mask's length.
- not-advertise - Suppresses routes that match the specified prefix/mask pair. This keyword applies to OSPF only.
- nssa-only - Sets the nssa-only attribute for the summary route (if any) generated for the specified prefix, which limits the summary to not-so-stubby-area (NSSA) areas.

Default Configuration

This command behavior is disabled by default.

Command Mode

Router RIP Configuration mode

User Guidelines

Routes learned from other routing protocols can be summarized. The metric used to advertise the summary is the lowest 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 0.0.0.0` command.

Example

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:

```
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# summary-address 10.1.0.0 255.255.0.0
switchxxxxxx(config-ospf)# exit
```

36.50. timers lsa arrival

To set the minimum interval at which the software accepts the same link-state advertisement (LSA) from OSPF neighbors, use the `timers lsa arrival` command in router configuration mode. To restore the default value, use the no form of this command.

Syntax

- timers lsa arrival milliseconds
- no timers lsa arrival

Parameters

- milliseconds - Minimum delay in milliseconds that must pass between acceptance of the same LSA arriving from neighbors. The range is 0 to 600,000 milliseconds. The default is 1000 milliseconds.

Default Configuration

1000 milliseconds

Command Mode

Router RIP Configuration mode

User Guidelines

The timers lsa arrival command controls the minimum interval for accepting the same LSA. The "same LSA" is defined as an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the LSA is dropped.

We suggest you keep the milliseconds value of the timers lsa arrival command less than or equal to the neighbors' hold-interval value of the timers throttle lsa all command.

Example

The following example sets the minimum interval for accepting the same LSA at 2000 milliseconds:

```
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# log-adjacency-changes
switchxxxxxx(config-ospf)# timers throttle lsa all 200 10000 45000
switchxxxxxx(config-ospf)# timers lsa arrival 2000
```

```
switchxxxxxx(config-ospf)# network 10.10.4.1  area 24
switchxxxxxx(config-ospf)# network 10.10.24.4 area 24
switchxxxxxx(config-ospf)# exit
```

37. PHY Diagnostics Commands

37.1. test cable-diagnostics tdr

To use Time Domain Reflectometry (TDR) technology to diagnose the quality and characteristics of a copper cable attached to a port, use the `test cable-diagnostics tdr` Privileged EXEC mode command.

Syntax

- test cable-diagnostics tdr interface interface-id

Parameters

- interface-id - (Optional) Specifies an Ethernet port ID.

Command Mode

Privileged EXEC mode

User Guidelines

This command does not work on fiber ports (if they exist on the device). The port to be tested should be shut down during the test, unless it is a combination port with fiber port active. In this case, it does not need to be shut down, because the test does not work on fiber ports.

The maximum length of cable for the TDR test is 120 meters.

Examples

Example 1 - Test the copper cables attached to port te1/0/1 (a copper port).

```
switchxxxxxx# test cable-diagnostics tdr interface te1/0/1
Cable is open at 64 meters
```

37.2. show cable-diagnostics tdr

To display information on the last Time Domain Reflectometry (TDR) test performed on all copper ports or on a specific copper port, use the `show cable-diagnostics tdr` Privileged EXEC mode command.

Syntax

- show cable-diagnostics tdr [interface interface-id]

Parameters

- interface-id - (Optional) Specify an Ethernet port ID.

Command Mode

Privileged EXEC mode

User Guidelines

The maximum length of cable for the TDR test is 120 meters.

Example

The following example displays information on the last TDR test performed on all copper ports.

```
switchxxxxxx# show cable-diagnostics tdr
      Port  Result      Length      Date
```

```
      ----  --------     [meters]     ------------------
------------
te1/0/1 OK
      te1/0/2 Short      50    13:32:00 23 July 2010
te1/0/3 Test has not been performed
      te1/0/4 Open       64    13:32:00 23 July 2010
```

37.3. show cable-diagnostics cable-length

To display the estimated copper cable length attached to all ports or to a specific port, use the `show cable-diagnostics cable-length` Privileged EXEC mode command.

Syntax

- show cable-diagnostics cable-length [interface interface-id]

Parameters

- interface-id - (Optional) Specify an Ethernet port ID.

Command Mode

Privileged EXEC mode

User Guidelines

The port must be active and working at 100 M or 1000 M.. The cable length results provided with this command may be effected if Green Ethernet Short Reach feature is enabled on the interface

Example

The following example displays the estimated copper cable length attached to all ports.

```
switchxxxxxx# show cable-diagnostics cable-length
Port     Length [meters]
-------- ---------------
te1/0/1  < 50
te1/0/2  Copper not active
te1/0/3  110-140
```

37.4. show fiber-ports optical-transceiver

To display the optical transceiver diagnostics, use the `show fiber-ports optical-transceiver` Privileged EXEC mode command.

Syntax

- show fiber-ports optical-transceiver [interface interface-id]

Parameters

- interface-id - (Optional) Specify an Ethernet port ID.

Default Configuration

All ports are displayed. If detailed is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show fiber-ports optical-transceiver
 Port Temp Voltage Current Output Input LOS
 [C] [Volt] [mA] Power Power
  [mWatt] [mWatt]
----------- ------ ------- ------- ------- ------- --
te1/0/1 Copper
te1/0/2 Copper
 te1/0/3 28 3.32 7.26 3.53 3.68 No te1/0/4 29 3.33 6.50 3.53 3.71 No
 Temp - Internally measured transceiver temperature
 Voltage - Internally measured supply voltage
 Current - Measured TX bias current
 Output Power - Measured TX output power in milliWatts
 Input Power - Measured RX received power in milliWatts
 LOS - Loss of signal
N/A - Not Available, N/S - Not Supported, W - Warning, E - Error
```

38. Power over Ethernet (PoE) Commands

38.1. power inline

To configure the inline power administrative mode on an interface, use the `power inline` Interface Configuration mode command.

Syntax

- power inline auto [time-range time-range-name] power inline never

Parameters

- auto - Turns on the device discovery protocol and applies power to the device.
- never - Turns off the device discovery protocol and stops supplying power to the device.
- time-range-name - Specifies a time range. When the time range is not in effect the power is not supplied the attached device. If a time range is not specified, there is no time range bounded to the port. (Range: 1–32 characters)

Default Configuration

The default configuration is set to auto.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

The never parameter cannot be used with a time range.

Example

The following example turns on the device discovery protocol on port 4.

```
switchxxxxxx(config)# interface te1/0/4
switchxxxxxx(config-if)# power inline auto
```

38.2. power inline inrush test disable

To disable the inrush test (a hardware test that checks input surge current for PoE devices), use the `power inline inrush test disable` Global Configuration mode command. To enable the inrush test, use the no form of this command.

Syntax

- power inline inrush test disable
- no power inline inrush test disable

Parameters

N/A.

Default Configuration

Inrush test is enabled.

Command Mode

Global Configuration mode

Example

The following example disable inrush test.

```
switchxxxxxx(config)# power inline inrush test disable
```

38.3. power inline legacy support disable

To disable the legacy PDs support, use the `power inline legacy support disable` Global Configuration mode command. To enable the legacy support, use the no form of this command.

Syntax

- power inline legacy support disable
- no power inline legacy support disable

Parameters

N/A.

Default Configuration

Legacy support is enabled.

Command Mode

Global Configuration mode

Example

The following example disables legacy PDs support.

```
switchxxxxxx(config)# power legacy support disable
```

38.4. power inline powered-device

To add a description of the device type, use the `power inline powered-device` Interface Configuration mode command. To remove the description, use the no form of this command.

Syntax

- power inline powered-device pd-type
- no power inline powered-device

Parameters

- pd-type - Enters a comment or a description to assist in recognizing the type of the device attached to this interface. (Length: 1–24 characters)

Default Configuration

There is no description.

Command Mode

Interface (Ethernet) Configuration mode

Example

The following example adds the description 'ip phone' to the device connected to port 4.

```
switchxxxxxx(config)# interface te1/0/4
switchxxxxxx(config-if)# power inline powered-device ip_phone
```

38.5. power inline priority

To configure the interface inline power management priority, use the `power inline priority` Interface Configuration (Ethernet) mode command. To restore the default configuration, use the no form of this command.

Syntax

- power inline priority {critical | high | low}
- no power inline priority

Parameters

- critical - Specifies that the device operation is critical.
- high - Specifies that the device operation is high priority.
- low - Specifies that the device operation is low priority.

Default Configuration

The default configuration is set to low priority.

Command Mode

Interface (Ethernet) Configuration mode

Example

The following example sets the inline power management priority of port `te1/0/4` to High.

```
switchxxxxxx(config)# interface te1/0/4
switchxxxxxx(config-if)# power inline priority high
```

38.6. power inline usage-threshold

To configure the threshold for initiating inline power usage alarms, use the `power inline usage-threshold` Global Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- power inline usage-threshold percent
- no power inline usage-threshold

Parameters

- percent - Specifies the threshold in percent to compare to the measured power. (Range: 1–99)

Default Configuration

The default threshold is 95 percent.

Command Mode

Global Configuration mode

Example

The following example configures the threshold for initiating inline power usage alarms to 90 percent.

```
switchxxxxxx(config)# power inline usage-threshold 90
```

38.7. power inline traps enable

To enable inline power traps, use the `power inline traps enable` Global Configuration mode command. To disable traps, use the no form of this command.

Syntax

- power inline traps enable
- no power inline traps enable

Default Configuration

Inline power traps are disabled.

Command Mode

Global Configuration mode

Example

The following example enables inline power traps.

```
switchxxxxxx(config)# power inline traps enable
```

38.8. power inline limit

To configure the power limit per port on an interface, use the `power inline limit` Interface Configuration mode command. To return to default, use the no form of the command.

Syntax

- power inline limit power
- no power inline limit

Parameters

- power - States the port power consumption limit in Milliwatts, Range is 0- 30000 .

Default Configuration

The default value is 30W

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

The operational power limit is the minimum of the configured power limit value and the maximum power capability on port. For example, if the configured value is higher than 15.4W on a PoE port, the operational power limit is 15.4W.

Example

The following example sets inline power on a port.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# power inline limit 2222
```

38.9. power inline limit-mode

To set the power limit mode of the system, use the `power inline limit-mode` Global Configuration mode command. To return to default, use the no form of this command.

Syntax

- power inline limit-mode {class | port}
- no power inline limit-mode

Parameters

- class - The power limit of a port is based on the class of the PD (Power Device) as detected during the classification process
- port - The power limit of a port is fixed regardless of the class of the discovered PD.

Default Configuration

The default value is port

Command Mode

Global Configuration mode

User Guidelines

Changing the PoE limit mode of the system will turn the power OFF and ON for all PoE ports.

Example

The following example sets the power limit to class.

```
switchxxxxxx(config)# power inline limit-mode class
"Changing the PoE limit mode of the system will turn the power OFF and ON for
all
PoE ports. Are you sure? [y/n]"
```

38.10. show power inline

To display information about the inline power for all interfaces or for a specific interface, use the `show power inline` privileged EXEC mode command.

Syntax

- show power inline [interface-id]

Parameters

- interface-id - Specifies an interface ID. The interface ID must be an Ethernet port.

Default Configuration

Show information for all ports.

Command Mode

Privileged EXEC mode

Examples

Example 1 - The following example displays information about the inline power for all ports (port power based).

```
switchxxxxxx(config)# show power inline
Port limit mode: Enabled
Usage threshold: 95%
Trap: Enabled
Legacy Mode: Disabled
Inrush test: Enabled
SW Version: 1.222.3.44
```

```
Unit Module Nominal Consumed Temp PSE chipset HW Revision
 power (w) Power (w) (c)
---- ------ --------- -------- ----- --- ------- -------------
1 48P 320 120 (37.5%) 30 PD69208 - 0x4BC2 PD69204 - 0x4AC2
2 24P 240 0 (0%) 50 PD69208 - 0x4AC2
3 24P 120 0 (0%) 50 PD69208 - 0x4AC2

Interface Admin Oper Power Class Device Priority
--------- ----- ---------- ----- ---------- ------------
te1/0/1 Auto On 15.4(3 0) 3 IP Phone Model A Critical
te1/0/2 Auto Searching 0 0 High
te1/0/3 Never Off 0 0 Low
```

Example 2 - The following example displays information about the inline power for a specific port.

```
switchxxxxxx(config)# show power inline te1/0/1
Interface   Admin Oper  Power Class Device      Priority
-------- --------- ----------- --------    ------- ------------------- ----
------
      -     --    -     -
      te1/0/1     Auto  On    3     IP Phone Model A  Critical
Port status: Port is on - Valid PD resistor signature detected
Port standard: 802.3AT Admin power limit: 30.0 watts Time range:
Link partner standard: 802.3AF
Operational power limit: 30 watts
Negiotiated power: 18 watts (LLDP)
#EDITOR: Power negotiation is done via LLDP . In case there was no power
negotiation with PD, the display of protocol type will be (none). In case there
was power negotiation, but it did not end in allocation of power by PSE, display
will be "0 watts (LLDP)" (power could still be allocated by Hardware). In case
negotiation has expired, the word "Expired" will be added, with the latest value
that was negotiated (e.g. "20Watts (LLDP - Expired)").
Current (mA): 81 Voltage(V): 50.8 verload Counter: 5 Short Counter: 0
Denied Counter: 2
Absent Counter: 0
Invalid Signature Counter: 0
```

The following table describes the fields shown in the display:

Field	Description
Power	Inline power sourcing equipment operational status.
Nominal Power	Inline power sourcing equipment nominal power in Watts.
Consumed Power	Measured usage power in Watts.
Usage Threshold	Usage threshold expressed in percent for comparing the measured power and initiating an alarm if threshold is exceeded.
Traps	Indicates if inline power traps are enabled.
Port	Ethernet port number.
device	Description of the device type.

State	Indicates if the port is enabled to provide power. The possible values are Auto or Never.
Priority	Port inline power management priority. The possible values are Critical, High or Low.
Status	Power operational state. The possible values are On, Off, Test-Fail, Testing, Searching or Fault.
Class	Power consumption classification of the device.
Overload Counter	Counts the number of overload conditions detected.
Short Counter	Counts the number of short conditions detected.
Denied Counter	Counts the number of times power was denied.
Absent Counter	Counts the number of times power was removed because device dropout was detected.
Invalid Signature Counter	Counts the number of times an invalid signature of a device was detected.
Inrush Test	Displays whether the inrush test is enabled or disabled.
Field	Description
Port limit mode	Enabled for port limit and Disable for class limit.
Legacy Mode	Enabled of Disabled legacy device support.
Inrush Test	Displays whether the inrush test is enabled or disabled.
SW version	The POE firmware version.
HW Version	The POE hardware version
Usage Threshold	Usage threshold expressed in percent for comparing the measured power and initiating an alarm if threshold is exceeded.
Traps	Indicates if inline power traps are enabled.
Module	The module name.
Available Power	Inline power sourcing equipment nominal power in Watts.
Consumed Power	Measured usage power in Watts.
Temp	Show the POE device temperature.
Interface	Ethernet port number.
Admin	Indicates if the port is enabled to provide power. The possible values are Auto or Never.
Oper	Power operational state. The possible values are On, Off, Test-Fail, Testing, Searching or Fault.
Power	Power consumed in watts.
Class	Power consumption classification of the device (0-4).

Device	Description of the device type set by the user.
Priority	Port inline power management priority. The possible values are Critical, High or Low.
Port status	The port status on/off with detailed reason (see bellow for details).
Port standard	802.3AF /802.3AT .
Admin power limit	Port limit in watts used when the Port limit mode is Enabled.
Time Range	The name of the time range associated with the interface.
Link partner standard	802.3AF/802.3AT.
Operational Power Limit	Port actual power limit in watts.
Current (mA)	Port current in Milli-Ampere.
Voltage (V)	Port voltage in volts.
Overload Counter	Counts the number of overload conditions detected.
Short Counter	Counts the number of short conditions detected.
Field	Description
Denied Counter	Counts the number of times power was denied.
Absent Counter	Counts the number of times power was removed because device dropout was detected.
Invalid Signature Counter	Counts the number of times an invalid signature of a device was detected.

Following is a list of port status values:

- Port is on - Valid capacitor/resistor detected.
- Port is on - Valid resistor/capacitor detected.
- Port is off - Main supply voltage is high.
- Port is off - Main supply voltage is low.
- Port is off - Hardware pin disables all ports.
- Port is off - User setting.
- Port is off - Detection is in process.
- Port is off - Non-802 - 3af powered device.
- Port is off - Overload & Underload states.
- Port is off - Underload state.
- Port is off - Overload state.
- Port is off - Power budget exceeded.
- Port is off - Voltage injection into the port.
- Port is off - Improper Capacitor Detection results.
- Port is off - Discharged load.
- Port is on - Detection regardless (Force On).
- Port is off - Forced power error due to Overload.
- Port is off - Out of power budget while in Force On.
- Port is off - Short condition.
- Port is off - Over temperature at the port.
- Port is off - Device is too hot.

- Port is off - Class Error - Illegal class.

39. Port Channel Commands

39.1. channel-group

To associate a port with a port-channel, use the `channel-group` Interface (Ethernet) Configuration mode command. To remove a port from a port-channel, use the no form of this command.

Syntax

- channel-group port-channel mode {on | auto}
- no channel-group

Parameters

- port-channel - Specifies the port channel number for the current port to join.
- mode - Specifies the mode of joining the port channel. The possible values are:
  - on - Forces the port to join a channel without an LACP operation.
  - auto - Forces the port to join a channel as a result of an LACP operation.

Default Configuration

The port is not assigned to a port-channel.

Command Mode

Interface (Ethernet) Configuration mode Default mode is on.

User Guidelines

LACP starts to manage port joining.

When the auto mode is configured and there are not received LACP messages on all port-candidates then one of candidates is joined. When the first LACP message is received the port is disjoined and LACP starts to manage port joining.

Example

The following example forces port `te1/0/1` to join port-channel 1 without an LACP operation.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# channel-group 1 mode on
```

39.2. port-channel load-balance

To configure the load balancing policy of the port channeling, use the `port-channel load-balance` Global Configuration mode command. To reset to default, use the no form of this command.

Syntax

- port-channel load-balance {src-dst-mac | src-dst-mac-ip}
- no port-channel load-balance

Parameters

- src-dst-mac - Port channel load balancing is based on the source and destination MAC addresses.
- src-dst-mac-ip - Port channel load balancing is based on the source and destination of MAC and IP addresses.

Default Configuration

src-dst-mac is the default option.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# port-channel load-balance src-dst-mac
```

39.3. show interfaces port-channel

To display port-channel information for all port channels or for a specific port channel, use the `show interfaces port-channel` Privileged EXEC mode command.

Syntax

- show interfaces port-channel [interface-id]

Parameters

- interface-id - (Optional) Specify an interface ID. The interface ID must be a port channel.

Command Mode

Privileged EXEC mode

Examples

The following example displays information on all port-channels.

switchxxxxxx# show interfaces port-channel

```
Load balancing: src-dst-mac.
Gathering information...
Channel Ports
------- -----
Po1 Active: 1,Inactive: te1/0/2-3
Po2 Active: 5 Inactive: te1/0/4
```

40. File System Commands

40.1. file Specification

The files may be located on:

- Network: TFTP servers and/or SCP servers - Network files
- FLASH - Flash files
- mass-storage connected to a USB port - USB files. Only one mass-storage is supported.

Uniform Resource Locators (URLs) are used to specify the location of a file or a directory. The URL has the following syntax:

<url> ::= tftp://<location>/<file-path> |
scp://[<username>:<password>@]<location>/<file-path> | usb://<file-path> |

flash://<file-path> | <current-directory>[/<file-path>] |

<higher-directory>[/<file-path>] | <file-path>

<username> ::= string up to 70 characters

<password> :: = string up to 70 characters

<location> ::= <ipv4-address> | <ipv6-address> | <dns-name>

<current-directory> ::= [{usb | flash}:][.]

<higher-directory> ::= [{usb | flash}:]..

<file-path> ::= [<directories-path>/]<filename>

<directories-path> ::= <directory-name> | <directories-path>/<directory-name>

The maximum number of directories in <directories-path> is 16.

<directory-name> ::= string up to 63 characters

<filename> ::= string up to 64 characters

Filenames and directory names consist only of characters from the portable filename character set. The set includes the following characters:

- A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
- a b c d e f g h i j k l m n o p q r s t u v w x y z
- <space>
- 0 1 2 3 4 5 6 7 8 9 . _ -

The last three characters are the <period>, <underscore>, and <hyphen> characters, respectively. If an URL includes spaces it must be enclosed by the " characters.

For example:

"flash://aaa it/alpha/file 125"

The maximal length of URL is 160 characters The following File systems are supported on USB:

- FAT32 - Full support.
- NTFS - Partially support: read only.

The switch supports the following predefined URL aliases:

- active-image - The predefined URL alias specifies the Active Image file.

This file has the following permissions:

- readable
- executable

- inactive-image - The predefined URL alias specifies the Inactive Image file. This file has the following permissions:
  - readable
  - executable
- running-config - The predefined URL alias specifies the Running Configuration File.
- startup-config - The predefined URL alias specifies the Startup Configuration File. This file has the following permissions:
  - readable
- localization. The predefined URL alias specifies the Secondary Language Dictionary file. This file has the following permissions:
  - readable
- logging. The predefined URL alias specifies the Syslog file. This file has the following permissions:
  - readable
- mirror-config. The predefined URL alias specifies the Mirror Configuration file. This file has the following permissions:
  - readable

Example

Example 1. The following example specifies a file on TFTP server using an IPv4 address:

```
tftp://1.1.1.1/aaa/dat/file.txt
```

Example 2. The following example specifies a file on TFTP server using an IPv6 address:

```
tftp://3000:1:2::11/aaa/dat/file.txt
```

Example 3. The following example specifies a file on TFTP server using a DNS name:

```
tftp://files.export.com/aaa/dat/file.txt
```

Example 4. The following example specifies a file on FLASH:

```
flash://aaa/dat/file.txt
```

Example 5. The following example specifies files using the current directory:

```
./dat/file.txt
dat/file.txt
```

Example 6. The following example specifies a file using the higher directory:

```
../dat/file.txt
```

Example 7. The following example specifies a file on mass-storage device connected to the USB port:

```
usb://aaa/dat/file.txt
```

Example 8. The following example specifies files on mass-storage device connected to the USB port using the current directory:

```
usb:aaa/dat/file.txt usb:./aaa/dat/file.txt
```

Example 9. The following example specifies a file on mass-storage device connected to the USB port using the higher directory:

```
usb:../aaa/dat/file.txt
```

40.2. system Flash Files

The system files used by the switch are in the flash://system/ directory. A user cannot add, delete, and rename the system files and directories, a user cannot create new directories under the system directory.

The system files are divided to the following groups:

- Inner System files. The files are created by the switch itself. For example the Syslog file.
- Files installed/Uninstalled by user. This group includes the following files:
  - Active and Inactive Images
  - Startup Configuration
  - Secondary Language Dictionary

The following boot commands install/uninstall these files:

- boot config
- boot localization
- boot system

Additionally, the following commands from previous versions can be used too:

- `copy` (copy running-config startup-config)
- write

Note. Reset to Factory Default removes all files from the FLASH except the following files:

- active-image
- inactive-image
- mirror-config
- localization

The flash://system/ directory contains the following directories:

- flash://system/images/ - The directory contains the Active and Inactive Image files.
- flash://system/configuration/ - The directory contains the Startup and Mirror Configuration files.
- flash://system/localization/ - The directory contains the Secondary Language Dictionary file.
- flash://system/syslog/ - The directory contains the Syslog file.
- flash://system/applications/ - The directory contains inner system files managed by the switch applications.

40.3. boot config

To install a file as Startup Configuration after reload, use the `boot config` command in Privileged EXEC mode. To uninstall the Startup configuration file, use the no form of this command.

Syntax

- boot config startup-config-url boot config running-config
- no boot config

Parameters

- startup-config-url - the url of a file. The predefined URLs cannot be configured.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

Use the `boot config startup-config-url` command to install Startup Configuration from the startup-config-url file. The file must be a text file containing CLI commands. The command performs the following actions:

- Copies the file into the system directory flash://system/configuration/
- Converts the file format from the text format in the inner binary format.
- Installs the converted file as Startup Configuration. The previous Startup Configuration file is deleted.

Use the `boot config running-config` command to install Startup Configuration from Running Configuration.

Use the no boot config command, to uninstall Startup Configuration. The uninstalled file is deleted.

Example

Example 1. The following example installs Startup Configuration from a TFTP server:

```
switchxxxxxx(config)# boot config tftp://1.1.1./confiration-files/config-
v1.9.dat
```

Example 2. TThe following example installs Startup Configuration from FLASH:

```
switchxxxxxx(config)# boot config flash://confiration-files/config-v1.9.dat
```

Example 3. The following example unsets the current Startup Configuration:

```
switchxxxxxx(config)# no boot config
```

Example 4. The following example installs Startup Configuration from the Running Configuration file:

```
switchxxxxxx(config)# boot config running-confg
```

40.4. boot localization

To install a file as the Secondary Language Dictionary file, use the `boot localization` command in Privileged EXEC mode. To return to the default, use the no form of this command.

Syntax

- boot localization dictionary-url
- no boot localization

Parameters

- dictionary-url - the url of a file. The predefined URLs cannot be configured.

Default Configuration

Default language.

Command Mode

Privileged EXEC mode

User Guidelines

Use the `boot dictionary dictionary-url` command to install Secondary Language Dictionary from the dictionary-url file. The command performs the following actions:

- Copies the file into the system directory flash://system/localization/
- Validates its format. If the file does not have the correct format the file is deleted and the command is finished with an error.
- Installs the copied file as Secondary Language Dictionary. The previous Secondary Language Dictionary file is deleted.

Use the no boot dictionary command, to uninstall Secondary Language Dictionary. The uninstalled file is deleted.

Example

Example 1. The following example installs the Secondary Language Dictionary file from a TFTP server:

```
switchxxxxxx(config)# boot localization tftp://196.1.1.1/web-
dictionaries/germany-dictionary.dat
```

Example 2. The following example installs the Secondary Language Dictionary file from FLASH:

```
switchxxxxxx(config)# boot localization flash://web-dictionaries/germany-
dictionary.dat
```

40.5. boot system

To install the system (active) image that the switch loads at startup, use the `boot system` command in Privileged EXEC mode.

Syntax

- boot system image-url
- boot system inactive-image

Parameters

- image-url - The URL of a file. The predefined URLs cannot be configured.

Default Configuration

No default.

Command Mode

Privileged EXEC mode

User Guidelines

Use the `boot system image-url` command to install a new active image from the image-url file. The command performs the following actions:

- Copies the file into the system directory flash://system/image/
- Validates its format. If the file does not have the correct image format the file is deleted and the command is finished with an error.
- Installs the copied file as the active image that will be used be loaded at startup. The previous active image file is save as inactive image. The previous inactive image is deleted.

Use the `boot system inactive-image` command to set the inactive image as active one and the active image as inactive one.

Use the `show bootvar / show version` command to display information about the active and inactive images.

Example

Example 1. The following example sets a new active image from a TFTP server:

```
switchxxxxxx(config)# boot system tftp://145.21.2.3/image/image-v1-1.ros
```

Example 2. The following example sets a new active image from FLASH:

```
switchxxxxxx(config)# boot system flash://images/image-v1-1.ros
```

Example 3. The following example sets the inactive image:

```
switchxxxxxx(config)# boot system inactive-image
```

40.6. cd

To change the current directory or file system, use the `cd` command in User EXEC mode.

Syntax

- cd url

Parameters

- url - Specifies a directory on FLASH or on USB.

Default Configuration

The flash root directory (flash://)

Command Mode

User EXEC mode

User Guidelines

When a terminal session is started the current directory of the session is set to flash://. Use the `cd` command to change the current directory.

Example

Example 1. The following example sets a new current directory on FLASH:

```
switchxxxxxx> pwd flash://
switchxxxxxx> cd date/aaa
switchxxxxxx> pwd
flash://date/aaa
```

Example 2. The following example sets a new current directory on USB:

```
switchxxxxxx> pwd flash://
switchxxxxxx> cd usb://
switchxxxxxx> pwd usb://
```

40.7. copy

To copy any file from a source to a destination, use the `copy` command in Privileged EXEC mode.

Syntax

- copy src-url dst-url
- copy src-url running-config
- copy running-config startup-config

Parameters

- src-url - The location URL of the source file to be copied. The predefined URL aliases can be configured.
- dst-url - The URL of the destination file or the directory to be copied. The predefined URL aliases cannot be configured.

Command Mode

Privileged EXEC mode

User Guidelines

The following guidelines are relevant:

- You cannot copy one network file to another network file.
- Use the copy src-url dst-url command to copy any file. If the dst-url argument defines an existed flash file the command fails if this file does not have the writable permission. If the dst-url argument defines a directory file then the file is copied into the directory with the same name. No file format validation or conversion is performed. If the src-url argument and dst-url arguments define flash files the dst-url file will have the permissions of the

src-url file. If the src-url argument defines a non-flash file and the dst-url argument defines a flash files the dst-url file will have the following permissions: - readable

- writable

- Use the copy src-url running-config command to add a file to the Running Configuration file.
- The copy running-config startup-config command has exactly the same functionality as the `boot config` command with the running-config keyword.

Example

Example 1. The following example copies file file1 from the TFTP server 172.16.101.101 to the flash://aaaa/file1 file:

```
switchxxxxxx# copy tftp://172.16.101.101/file1 flash://aaa/file1
```

Example 2. The following example saves the Startup configuration file in the tftp://172.16.101.101/config.txt file:

```
switchxxxxxx# copy startup-config tftp://172.16.101.101/config.txt
```

Example 3. The following example copies the Running Configuration file to the Startup configuration:

```
switchxxxxxx# copy running-config startup-config
```

Example 4. The following example copies the Syslog file to a TFTP server:

```
switchxxxxxx# copy logging tftp://1.1.1.1/syslog.txt
```

Example 5. The following example copies a file from the mass-storage device connected to the USB port to Flash:

```
switchxxxxxx# copy usb://aaa/file1.txt flash://dir1/file2
```

40.8. delete

To delete a local file, use the `delete` command in Privileged EXEC mode.

Syntax

- delete <url>
- delete <file-name>
- delete [startup-config|localization]

Parameters

- url - Specifies the local URL of the local file to be deleted. The predefined and network URLs cannot be configured.
- file-name - Specifies the name of SNA user file to delete.

Command Mode

Privileged EXEC mode

User Guidelines

The delete url command cannot delete a network file.

Use the delete startup-config command to delete the Startup Configuration file.

Use the delete localization command to delete the Secondary Language Dictionary file.

Example

Example 1. The following example deletes the file called 'backup/config' from FLASH:

```
switchxxxxxx# cd flash://backup/
switchxxxxxx# delete aaa.ttt
Delete flash://backup/aaa.ttt? [Y/N]Y
```

Example 2. The following example deletes the file called 'aaa/config' from the mass-storage device connected to the USB port:

```
switchxxxxxx# delete usb://aaa/config
Delete usb://aaa/config? [Y/N]Y
```

40.9. dir

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

Syntax

- dir [url]

Parameters

- url - Specifies the local URL of the directory to be displayed. The predefined and network URLs cannot be configured. If the argument is omitted the current directory is used.

Command Mode

User EXEC mode

User Guidelines

The command cannot be applied to a network directory.

Use the dir command without the argument to display the current directory.

Examples

The following example displays the flash://mng/ directory:

```
switchxxxxxx> dir flash://mng/ Permissions d-directory r-readable w-writable x-
executable
134560K of 520000K are free
Directory of flash://mng/
Permission File Size Last Modified File Name
---------- --------- ------------------- -----------------
drw- 4720148 Dec 12 2010 17:49:36 bin
-r-- 60 Dec 12 2011 17:49:36 config-list
-r-- 160 Feb 12 2011 17:49:36 image-list
-r-x 6520148 Nov 29 2010 7:12:30 image1
-rw- 2014 Nov 20 2010 9:12:30 data
```

40.10. mkdir

To create a new directory, use the `mkdir` command in Privileged EXEC mode.

Syntax

- mkdir url

Parameters

- url - Specifies the URL of the created directory. The predefined and network URLs cannot be configured.

Command Mode

Privileged EXEC mode

User Guidelines

The mkdir command cannot be applied to a network directory.

The mkdir command cannot create a directory into the flash://system/ directory.

All directories defined in the url argument except the created one must exist.

Example

Example 1. The following example creates a directory on FLASH:

```
switchxxxxxx# mkdir flash://date/aaa/
```

Example 2. The following example creates a directory on the mass-storage device connected to the USB port:

```
switchxxxxxx# mkdir usb://newdir/
```

40.11. more

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

Syntax

- more url

Parameters

- url - Specifies the local URL or predefined file name of the file to display.

Command Mode

User EXEC mode

User Guidelines

The command cannot be applied to a network file.

The more running-config command displays the same output as the `show running-config` command regardless the specified format.

The more startup-config command displays the same output as the `show startup-config` command regardless the specified format.

The more active-image and more inactive-image commands display only the version number of the image regardless the specified format.

Example

The following example displays the running configuration file contents:

```
switchxxxxxx> more running-config no spanning-tree interface range gi/11-48
speed 1000 exit no lldp run line console exec-timeout 0
```

40.12. pwd

To show the current directory, use the `pwd` command in User EXEC mode.

Syntax

- pwd [usb: | flash:]

Parameters

- usb: - Display the current directory on the USB driver.
- flash: - Display the current directory on the FLASH driver.

Command Mode

User EXEC mode

User Guidelines

Use the pwd usb: I flash: command to show the current directory on the specified driver.

Use the pwd command to show the current directory set by the recent cd command.

Example

The following example uses the cd command to change the current directory and then uses the pwd command to display that current directory:

```
switchxxxxxx> pwd flash://
switchxxxxxx> cd date/aaa
switchxxxxxx> pwd flash://date/aaa
```

40.13. reload

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

Syntax

- reload
- reload {in hhh:mm | mmm | at hh:mm [day month]}
- reload cancel

Parameters

- in hhh:mm | mmm - Schedules a reload of the image to take effect in the specified minutes or hours and minutes. The reload must take place within approximately 24 days.
- at hh:mm - Schedules a reload of the image to take place at the specified time (using a 24-hour clock). 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 (if the specified time is later than the current time) or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within 24 hours.
- day - Number of the day in the range from 1 to 31.
- month - Month of the year. (Range: Jan–Dec)
- cancel - Cancels a scheduled reload.

Command Mode

Privileged EXEC mode

User Guidelines

Use the reload command to reload the switch.

Use the reload {in hhh:mm | mmm | at hh:mm [day month]} command the command to specify scheduled switch reload.

The at keyword can be configured only if the system clock has been set on the switch.

When you specify the reload time using the at keyword, if you specify the month and day, the reload takes 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 (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within 24 days.

Use the reload cancel command to cancel the scheduled reload.

To display information about a scheduled reload, use the `show reload` command.

Example

Example 1. The following example reloads the switch:

```
switchxxxxxx# reload
This command will reset the whole system and disconnect your current session.
Do you want to continue? (Y/N) [Y]
```

Example 2. The following example reloads the image in 10 minutes:

```
switchxxxxxx# reload in 10
This command will reset the whole system and disconnect your current session.
Reload is scheduled for 11:57:08 UTC Fri Apr 21 2012 (in 10 minutes). Do you
want to continue? (Y/N) [Y]
```

Example 3. The following example reloads the image at 12:10 24 Aug:

```
switchxxxxxx# reload at 12:10 24 Aug
This command will reset the whole system and disconnect your current session.
Reload is scheduled for 12:10:00 UTC Sun Aug 24 2014 (in 1 hours and 12
minutes). Do you want to continue ? (Y/N)[N]
```

Example 4. The following example reloads the image at 13:00:

```
switchxxxxxx# reload at 13:00 soft
This command will reset the whole system and disconnect your current session.
Reload is scheduled for 13:00:00 UTC Fri Apr 21 2012 (in 1 hour and 3 minutes).
Do you want to continue? (Y/N) [Y]
```

Example 5. The following example cancels a reload.

```
switchxxxxxx# reload cancel Reload cancelled.
```

40.14. rename

To rename a local file or directory, use the `rename` command in Privileged EXEC mode.

Syntax

- rename url new-url

Parameters

- url - Specifies the URL of the file or directory to be renamed. The predefined and network URLs cannot be configured.
- new-url - Specifies the new URL of the renamed file or directory. The predefined and network URLs cannot be configured.

Command Mode

Privileged EXEC mode

User Guidelines

The url and new-url arguments must specifies the same driver.

The command cannot rename a network file or network directory.

The command cannot rename a file or directory into the flash://system directory.

Examples

Example 1. The following example renames the flash://bin/text1.txt file to flash://archive/text1sav.txt:

```
switchxxxxxx# cd flash://archive
switchxxxxxx# rename flash://bin/text1.txt ./text1sav.txt
```

Example 2. The following example renames the flash://a/b directory to the flash://e/g/h directory:

```
switchxxxxxx# pwd flash://a/b/c/d
switchxxxxxx> dir flash://a
Permissions
d-directory
r-readable
w-writable
x-executable
134560K of 520000K are free
Directory of flash://a
File Name Permission File Size Last Modified
--------- ---------- --------- -------------------
b drw- 472148 Dec 13 2010 15:49:36

switchxxxxxx> dir flash://e/g/h
Permissions
d-directory
r-readable
w-writable
x-executable
134560K of 520000K are free
Directory of flash://e/g/h
File Name Permission File Size Last Modified
--------- ---------- --------- -------------------
switchxxxxxx# rename flash://a/b flash://e/g/h
switchxxxxxx# pwd flash://e/g/h/c/d
switchxxxxxx> dir flash://a
Permissions
d-directory
r-readable
w-writable
x-executable
134560K of 520000K are free
Directory of flash://mng/
File Name Permission File Size Last Modified
--------- ---------- --------- -------------------
switchxxxxxx> dir flash://e/g/h
```

```
Permissions
d-directory
r-readable
w-writable
x-executable
134560K of 520000K are free
Directory of flash://e/g/h
File Name Permission File Size Last Modified
--------- ---------- --------- -------------------
c drw- 720148 Dec 12 2010 17:49:36
```

40.15. rmdir

To remove a local directory, use the `rmdir` command in Privileged EXEC mode.

Syntax

- rmdir url

Parameters

- url - Specifies the URL of the file or directory to be deleted. The predefined and network URLs cannot be configured.

Command Mode

Privileged EXEC mode

User Guidelines

Only empty directory can be deleted.

The command cannot remove a network directory.

The command cannot remove a directory into the flash://system directory.

Example

Example 1. The following example removes the directory called 'backup/config/' from FLASH:

```
switchxxxxxx# rmdir flash://backup/config/
Remove flash://backup/config? [Y/N]Y
```

Example 2. The following example removes the directory called 'aaa/config' from the mass-storage device connected to the USB port:

```
switchxxxxxx# rmdir usb://aaa/config/
Remove directory usb://aaa/config? [Y/N]Y
```

40.16. show bootvar / show version

To display the active system image file that was loaded by the device at startup, and to display the system image file that will be loaded after rebooting the switch, use the `show bootvar` or `show version` command in User EXEC mode.

Syntax

- show bootvar
- show version

Parameters

This command has no arguments or keywords.

Command Mode

User EXEC mode

User Guidelines

The show bootvar and show version commands have the same functionality.

Example

Example 1. The following example gives an example of the command output after reload:

```
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
 Version: 12.03
 MD5 Digest: 23FA000012857D8855AABC7577AB5562
 Date: 04-Jul-2014
 Time: 15:03:07
Inactive-image: flash://system/images/image_v12-01.ros
 Version: 12.01
 MD5 Digest: 3FA000012857D8855AABC7577AB8999
 Date: 04-Feb-2001
 Time: 11:13:17
```

Example 2. This example continues the inactive one, after applying the boot system tftp://1.1.1.1/image_v14-01.ros command:

```
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
 Version: 12.03
 MD5 Digest: 63FA000012857D8855AABEA7451265456
 Date: 04-Jul-2014
 Time: 15:03:07
 Inactive after reboot
Inactive-image: flash://system/images/image_v14-01.ros
 Version: 14.01
 MD5 Digest: 23FA000012857D8855AABC7577AB5562
 Date: 24-Jul-2014
 Time: 23:11:17
 Active after reboot
```

Example 3. This example continues the inactive one, after a system reload:

```
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v14-01.ros
 Version: 14.01
 MD5 Digest: 23FA000012857D8855AABC7577AB5562
 Date: 24-Jul-2014
 Time: 23:11:17
Inactive-image: flash://system/images/image_v12-03.ros
 Version: 12.03
 MD5 Digest: 63FA000012857D8855AABEA7451265456
 Date: 04-Jul-2014
 Time: 15:03:07
```

Example 4. This example continues the inactive one, after applying the boot system inactive-image command:

```
switchxxxxxx# show bootvar
```

```
Active-image: flash://system/images/image_v14-01.ros
 Version: 14.01
 MD5 Digest: 23FA000012857D8855AABC7577AB5562
 Date: 24-Jul-2014
 Time: 23:11:17
 Inactive after reboot
Inactive-image: flash://system/images/image_v12-03.ros
 Version: 12.03
 MD5 Digest: 63FA000012857D8855AABEA7451265456
 Date: 04-Jul-2014 Time: 15:03:07
Active after reboot
```

Example 5. This example continues the inactive one, after a system reload:

```
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
 Version: 12.03
 MD5 Digest: 63FA000012857D8855AABEA7451265456
 Date: 04-Jul-2014
 Time: 15:03:07
Inactive-image: flash://system/images/_image_v12-03.ros
 Version: 12.03
 MD5 Digest: 63FA000012857D8855AABEA7451265456
 Date: 04-Jul-2014
 Time: 15:03:07
```

Example 6. The following example gives an example of the command output after applying the boot system command two times:

```
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
 Version: 12.03
 MD5 Digest: 63FA000012857D8855AABEA7451265456
 Date: 04-Jul-2014
 Time: 15:03:07
Inactive-image: flash://system/images/image_v12-01.ros
 Version: 12.01
 MD5 Digest: 3FA000012857D8855AABC7577AB8999
 Date: 04-Feb-2001 Time: 11:13:17
switchxxxxxx# boot system tftp://1.1.1.1/image_v14-01.ros
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
 Version: 12.03
 MD5 Digest: 63FA000012857D8855AABEA7451265456
 Date: 04-Jul-2014
 Time: 15:03:07
 Inactive after reboot
Inactive-image: flash://system/images/image_v14-01.ros
 Version: 14.01
 MD5 Digest: 23FA000012857D8855AABC7577AB5562
 Date: 24-Jul-2014
 Time: 23:11:17 Active after reboot
switchxxxxxx# boot system tftp://1.1.1.1/image_v14-04.ros
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
 Version: 12.03
 MD5 Digest: 63FA000012857D8855AABEA7451265456
```

```
 Date: 04-Jul-2014
 Time: 15:03:07
 Inactive after reboot
Inactive-image: flash://system/images/image_v14-04.ros
 Version: 14.01
 MD5 Digest: 23FA000012857D8855AABC7577AB5562
 Date: 24-Jul-2014
 Time: 23:11:17
 Active after reboot
```

Example 7. The following example gives an example of the command output after applying the boot system tftp://1.1.1.1/image_v14-01.ros command and the boot system inactive-image command:

```
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
 Version: 12.03
 MD5 Digest: 63FA000012857D8855AABEA7451265456
 Date: 04-Jul-2014
 Time: 15:03:07
Inactive-image: flash://system/images/image_v12-01.ros
 Version: 12.01
 MD5 Digest: 3FA000012857D8855AABC7577AB8999
 Date: 04-Feb-2001 Time: 11:13:17
switchxxxxxx# boot system tftp://1.1.1.1/image_v14-01.ros
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
 Version: 12.03
 MD5 Digest: 63FA000012857D8855AABEA7451265456
 Date: 04-Jul-2014
 Time: 15:03:07
 Inactive after reboot
Inactive-image: flash://system/images/image_v14-01.ros
 Version: 14.01
 MD5 Digest: 23FA000012857D8855AABC7577AB5562
 Date: 24-Jul-2014
 Time: 23:11:17 Active after reboot
switchxxxxxx# boot system inactive-image
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
 Version: 12.03
 MD5 Digest: 63FA000012857D8855AABEA7451265456
 Date: 04-Jul-2014
 Time: 15:03:07
Inactive-image: flash://system/images/image_v14-01.ros
 Version: 14.01
 MD5 Digest: 23FA000012857D8855AABC7577AB5562
 Date: 24-Jul-2014
 Time: 23:11:17
```

40.17. show reload

To display the reload status on the switch, use the `show reload` command in User EXEC mode.

Syntax

- show reload

Parameters

This command has no arguments or keywords.

Command Mode

User EXEC mode

User Guidelines

You can use the `show reload` command to display a pending image reload. To cancel the reload, use the `reload` command with the cancel keyword.

Example

Example 1. The following example displays information when scheduled reload has been configured:

```
switchxxxxxx> show reload
Image reload scheduled for 00:00:00 UTC Sat April 20 (in 3 hours and 12 minutes)
```

Example 2. The following example displays information when scheduled reload has not been configured:

```
switchxxxxxx> show reload
No scheduled reload
```

40.18. show running-config

To display the contents of the currently running configuration file, use the `show running-config` command in Privileged EXEC mode.

Syntax

- show running-config [interface interface-id-list | detailed | brief]

Parameters

- interface interface-id-list - Specifies a list of interface IDs. The interface IDs can be one of the following types: Ethernet port, port-channel or VLAN.
- detailed - Displays configuration with SSL and SSH keys.
- brief - Displays configuration without SSL and SSH keys.

Default Configuration

All interfaces are displayed. If the detailed or brief keyword is not specified, the brief keyword is applied.

Command Mode

Privileged EXEC mode

Example

The following example displays the running configuration file contents.

```
switchxxxxxx# show running-config
config-file-header AA307-02
v1.2.5.76 / R750_NIK_1_2_584_002
CLI v1.0
```

```
no spanning-tree
interface range te1/0/1-4
speed 1000 exit
no lldp run
interface vlan 1
ip address 1.1.1.1 255.0.0.0
exit
line console
exec-timeout 0
exit
switchxxxxxx#
```

40.19. show startup-config

To display the Startup Configuration file contents, use the `show startup-config` command in Privileged EXEC mode.

Syntax

- show startup-config [interface interface-id-list]

Parameters

- interface interface-id-list - Specifies a list of interface IDs. The interface IDs can be one of the following types: Ethernet port, port-channel or VLAN.

Command Mode

Privileged EXEC mode

Example

The following example displays the startup configuration file contents.

```
switchxxxxxx# show startup-config
config-file-header
AA307-02 v1.2.5.76 / R750_NIK_1_2_584_002
CLI v1.0
no spanning-tree
interface range te1/0/1-4
speed 1000
exit
no lldp run
interface vlan 1
ip address 1.1.1.1 255.0.0.0
exit
ine console
exec-timeout 0
exit
switchxxxxxx#
```

40.20. write

To save the running configuration to the startup configuration file, use the `write` command in Privileged EXEC mode.

Syntax

- write
- write memory

Parameters

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

User Guidelines

Use the `write` command or the write memory command to save the Running Configuration file into the Startup Configuration file.

Examples

The following example shows how to overwrite the startup-config file with the running-config file with the write command.

```
switchxxxxxx# write
Overwrite file [startup-config] ?[Yes/press any key for no]....15-Sep-2010
11:27
:48 %COPY-I-FILECPY: Files Copy - source URL running-config destination URL
flash://startup-config
15-Sep-2010 11:27:50 %COPY-N-TRAP: The copy operation was completed successfully
Copy succeeded
```

41. Quality of Service (QoS) Commands

41.1. qos

Use the `qos` Global Configuration mode command to enable QoS on the device and set its mode. Use the no form of this command to disable QoS on the device.

Syntax

- qos [basic | {advanced [ports-not-trusted | ports-trusted]}|map]
- no qos

Parameters

- basic - QoS basic mode. If no option is specified, the QoS mode defaults to the basic mode.
- advanced - Specifies the QoS advanced mode, which enables the full range of QoS configuration.
- ports-not-trusted - Relevant for advanced mode only. Indicates that packets, which are not classified by policy map rules to a QoS action, are mapped to egress queue 0. This is the default setting in advanced mode.
- ports-trusted - Relevant for advanced mode only. Indicates that packets, which are not classified by policy map rules to a QoS action, are mapped to an egress queue based on the packet's fields. Use the `qos advanced-mode trust` command to specify the trust mode.
- map - configure the QoS maps.

Default Configuration

QoS basic mode

Command Mode

Global Configuration mode

Examples

Example 1 - The following example disables QoS on the device.

```
switchxxxxxx(config)# no qos
```

Example 2 - The following example enables QoS advanced mode on the device with the ports-not-trusted option.

```
switchxxxxxx(config)# qos advanced
```

41.2. qos advanced-mode trust

Use the `qos advanced-mode trust` Global Configuration mode command to configure the trust mode in advanced mode. Use the no form of this command to return to default.

Syntax

- qos advanced-mode trust {cos | dscp | cos-dscp}
- no qos advanced-mode trust

Parameters

- cos - Classifies ingress packets with the packet CoS values. For untagged packets, the port default CoS is used.

- dscp - Classifies ingress packets with the packet DSCP values.
- cos-dscp - Classifies ingress packets with the packet DSCP values for IP packets. For other packet types, use the packet CoS values.

Default Configuration

cos-dscp

Command Mode

Global Configuration mode

The configuration is relevant for advanced mode in the following cases:

- ports-not-trusted mode: For packets that are classified to the QoS action trust.
- ports-trusted mode: For packets that are not classified by to any QoS action or classified to the QoS action trust.

Example

The following example sets cos as the trust mode for QoS on the device.

```
switchxxxxxx(config)# qos advanced-mode trust cos
```

41.3. show qos

Use the `show qos` Privileged EXEC mode command to display the QoS information for the device. The trust mode is displayed for the QoS basic mode.

Syntax

- show qos

Parameters

N/A

Default Configuration

Disabled Command Mode

Command Mode

Privileged EXEC mode

User Guidelines

Trust mode is displayed if QoS is enabled in basic mode

Examples

```
switchxxxxxx(config)# show qos
Qos: Disabled
switchxxxxxx(config)# show qos
Qos: Basic mode Basic trust: dscp
switchxxxxxx(config)# show qos Qos: Advanced mode
Advanced mode trust type: cos
Advanced mode ports state: Trusted
```

41.4. class-map

Use the `class-map` Global Configuration mode command to create or modify a class map and enter the Class-map Configuration mode (only possible when QoS is in the advanced mode). Use the no form of this command to delete a class map.

Syntax

- class-map class-map-name [match-all | match-any]
- no class-map class-map-name

Parameters

- class-map-name - Specifies the class map name. (Length: 1–32 characters)
- match-all - Performs a logical AND of all the criteria of the ACLs belonging to this class map. All match criteria in this class map must be matched. If neither match-all nor match-any is specified, the match-all parameter is selected by default.
- match-any - Performs a logical OR of the criteria of the ACLs belonging to this class map. Only a single match criteria in this class map must be matched.

Default Configuration

No class map.

Command Mode

Global Configuration mode

The class-map command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally-named service policy applied on a per-interface basis.

A class map consists of one or more ACLs. It defines a traffic flow by determining which packets match some or all of the criteria specified in the ACLs.

All class map commands are only available when QoS is in advanced mode.

The class-map enters Class-map Configuration mode. In this mode, up to two match commands can be entered to configure the criteria for this class. Each match specifies an ACL.

When using a few match commands, each must point to a different type of ACL, such as: one IP ACL, one IPv6 ACL, and one MAC ACL. The classification is by first match, therefore, the order of the ACLs is important.

Error messages are generated in the following cases:

- There is more than one `match` command in a match-all class map
- There is a repetitive classification field in the participating ACLs.

After entering the Class-map Configuration mode, the following configuration commands are available:

- `exit`: Exits the Class-map Configuration mode.
- `match`: Configures classification criteria.
- `no`: Removes a match statement from a class map.

Example

The following example creates a class map called Class1 and configures it to check that packets match all classification criteria in the ACL specified.

```
switchxxxxxx(config)# class-map class1 match-all
switchxxxxxx(config-cmap)# match access-group acl-name
```

41.5. show class-map

The show class-map Privileged EXEC mode mode command displays all class maps when QoS is in advanced mode.

Syntax

- show class-map [class-map-name]

Parameters

- class-map-name - Specifies the name of the class map to be displayed. (Length: 1–32 characters)

Command Mode

Privileged EXEC mode

Example

The following example displays the class map for Class1.

```
switchxxxxxx(config)# show class-map
Class Map matchAny class1
 Match access-group mac
```

41.6. match

Use the `match` Class-map Configuration mode. command to bind the ACLs that belong to the class-map being configured. Use the no form of this command to delete the ACLs.

Syntax

- match access-group acl-name
- no match access-group acl-name

Parameters

- acl-name - Specifies the MAC, IP ACL name, or IPv6 ACL name. (Length: 1–32 characters)

Default Configuration

No match criterion is supported.

This command is available only when the device is in QoS advanced mode.

Command Mode

Class-map Configuration mode.

Example

The following example defines a class map called Class1. Class1 contains an ACL called enterprise. Only traffic matching all criteria in enterprise belong to the class map.

```
switchxxxxxx(config)# class-map class1
switchxxxxxx(config-cmap)# match access-group enterprise
```

41.7. policy-map

Use the `policy-map` Global Configuration mode command to creates a policy map and enter the Policy-map Configuration mode. Use the no form of this command to delete a policy map.

Syntax

- policy-map policy-map-name
- no policy-map policy-map-name

Parameters

- policy-map-name - Specifies the policy map name. (Length: 1–32 characters)

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

This command is only available when QoS is in advanced mode.

Use the policy-map Global Configuration mode command to specify the name of the policy map to be created, added to, or modified before configuring policies for classes whose match criteria are defined in a class map.

A policy map contains one or more class maps and an action that is taken if the packet matches the class map. Policy maps may be bound to ports/port-channels.

Entering the `policy-map` Global Configuration mode command also enables configuring or modifying the class policies for that policy map. Class policies in a policy map can be configured only if the classes have match criteria defined for them.

Policy map is applied on the ingress path.

The match criteria is for a class map. Only one policy map per interface is supported. The same policy map can be applied to multiple interfaces and directions.

The `service-policy` command binds a policy map to a port/port-channel.

Example

The following example creates a policy map called Policy1 and enters the Policy-map Configuration mode.

```
switchxxxxxx(config)# policy-map policy1
switchxxxxxx(config-pmap)#
```

41.8. class

Use the `class` Policy-map Configuration mode. command after the `policy-map` command to attach ACLs to a policy-map. Use the no form of this command to detach a class map from a policy map.

Syntax

- class class-map-name [access-group acl-name]
- no class class-map-name

Parameters

- class-map-name - Specifies the name of an existing class map. If the class map does not exist, a new class map is created under the specified name. (Length: 1–32 characters)
- access-group acl-name - Specifies the name of an IP, IPv6, or MAC Access Control List (ACL). (Length: 1–32 characters)

Default Configuration

No class map is defined for the policy map.

Command Mode

Policy-map Configuration mode.

User Guidelines

This command is only available when QoS is in advanced mode.

This is the same as creating a class map and then binding it to the policy map.

You can specify an existing class map in this command, or you can use the access-group parameter to create a new class map.

After the policy-map is defined, use the `service-policy` command to attach it to a port/port-channel.

Example

The following example defines a traffic classification (class map) called class1 containing an ACL called enterprise. The class is in a policy map called policy1. The policy-map policy1 now contains the ACL enterprise.

```
switchxxxxxx(config)# policy-map policy1
switchxxxxxx(config-pmap)# class class1 access-group enterprise
```

41.9. show policy-map

Use the `show policy-map` Privileged EXEC mode command to display all policy maps or a specific policy map.

This command is only available when QoS is in advanced mode.

Syntax

- show policy-map [policy-map-name]

Parameters

- policy-map-name - Specifies the policy map name. (Length: 1–32 characters)

Default Configuration

All policy-maps are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays all policy maps.

```
switchxxxxxx(config)# show policy-map
Policy Map policy1
class class1
set dscp 7 Po
licy Map policy2
class class 2 police 96000 4800 exceed-action drop
class class2
redirect te1/0/2
class class 3 police 96000 4800 exceed-action policed-dscp-transmit peak 128000
9600 violate-action policed-dscp-transmit
```

41.10. trust

Use the `trust` Policy-map Class Configuration mode. command to configure the trust state. Use the no form of this command to return to the default trust state.

Syntax

- trust
- no trust

Parameters

N/A

Default Configuration

The default state is according to the mode selected in the `qos` command (advanced mode). The type of trust is determined in `qos advanced-mode trust`.

Command Mode

Policy-map Class Configuration mode.

User Guidelines

This command is relevant only when QoS is in advanced, ports-not-trusted mode. Trust indicates that traffic is sent to the queue according to the packet’s QoS parameters (UP or DSCP).

Use this command to distinguish the QoS trust behavior for certain traffic from others. For example, incoming traffic with certain DSCP values can be trusted. A class map can be configured to match and trust the DSCP values in the incoming traffic.

The type of trust is determined in `qos advanced-mode trust`.

Trust values set with this command supersede trust values set on specific interfaces with the `qos trust (Interface)` Interface Configuration mode command.

The `trust` and `set` commands are mutually exclusive within the same policy map.

The set command is not supported into egress policies.

If specifying trust cos, QoS maps a packet to a queue, the received or default port CoS value, and the CoS-to-queue map.

Example

The following example creates an ACL, places it into a class map, places the class map into a policy map and configures the trust state.

```
switchxxxxxx(config)# ip access-list extended ip1
switchxxxxxx(config-ip-al)# permit ip any any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# class-map c1
switchxxxxxx(config-cmap)# match access-group ip1
switchxxxxxx(config-cmap)# exit
switchxxxxxx(config)# policy-map p1
switchxxxxxx(config-pmap)# class c1
switchxxxxxx(config-pmap-c)# trust
```

41.11. set

Use the `set` Policy-map Class Configuration mode. command to select the value that QoS uses as the DSCP value, the egress queue or to set user priority values.

Syntax

- set {dscp new-dscp | queue queue-id | cos new-cos}
- no set

Parameters

- dscp new-dscp - Specifies the new DSCP value for the classified traffic. (Range: 0–63)
- queue queue-id - Specifies the egress queue. (Range: 1-8)
- cos new-cos - Specifies the new user priority to be marked in the packet. (Range: 0–7)

Command Mode

Policy-map Class Configuration mode.

User Guidelines

This command is only available when QoS is in advanced mode.

The `set` and `trust` commands are mutually exclusive within the same policy map.

To return to the Configuration mode, use the `exit` command. To return to the Privileged EXEC mode, use the `end` command.

The queue keyword is not supported into egress policies.

Example

The following example creates an ACL, places it into a class map, places the class map into a policy map and sets the DSCP value in the packet to 56 for classes in the policy map called p1.

```
switchxxxxxx(config)# ip access-list extended ip1
switchxxxxxx(config-ip-al)# permit ip any any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# class-map c1
switchxxxxxx(config-cmap)# match access-group ip1
switchxxxxxx(config-cmap)# exit
switchxxxxxx(config)# policy-map p1
switchxxxxxx(config-pmap)# class c1
switchxxxxxx(config-pmap-c)# set dscp 56
```

41.12. redirect

Use the `redirect` Policy-map Class Configuration mode. command to redirect a traffic flow to a given Ethernet port or port channel.

Syntax

- redirect interface-id
- no redirect

Parameters

- interface-id - Specifies an Ethernet port or port channel to which the flow is redirected.

Command Mode

Policy-map Class Configuration mode.

User Guidelines

Use the `redirect` command to redirect a frame into the VLAN the frame was assigned to.

This command is only available when QoS is in advanced mode.

Example

The following example creates an ACL, places it into a class map, places the class map into a policy map and redirects the flow to Ethernet port te1/0/2:

```
switchxxxxxx(config)# ip access-list extended ip1
switchxxxxxx(config-ip-al)# permit ip any any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# class-map c1
switchxxxxxx(config-cmap)# match access-group ip1
switchxxxxxx(config-cmap)# exit
switchxxxxxx(config)# policy-map p1
switchxxxxxx(config-pmap)# class c1
switchxxxxxx(config-pmap-c)# redirect te1/0/2
switchxxxxxx(config-pmap-c)# exit
switchxxxxxx(config-pmap)# exit
switchxxxxxx(config)#
```

41.13. mirror

Use the `mirror` Policy-map Class Configuration mode. command to mirror a traffic flow to an analyzer Ethernet port.

Syntax

- mirror session_number
- no mirror

Parameters

- session_number - Specify the session number identified with the SPAN or RSPAN session. Only a value of 1 is allowed.

Command Mode

Policy-map Class Configuration mode.

User Guidelines

This command is only available when QoS is in advanced mode.

A frame is mirrored in the same format if it matches to one of the class ACLs regardless the command of this ACL: permit or deny.

Only one source session from VLAN and flow mirroring is supported.

The analyzer Ethernet port is configured by the `monitor session destination` command with the same session number.

Example

The following example creates an ACL, places it into a class map, places the class map into a policy map and mirrors the flow to an analyzer Ethernet port defined by session 2:

```
switchxxxxxx(config)# ip access-list extended ip1
switchxxxxxx(config-ip-al)# permit ip any any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# class-map c1
switchxxxxxx(config-cmap)# match access-group ip1
switchxxxxxx(config-cmap)# exit
switchxxxxxx(config)# policy-map p1
switchxxxxxx(config-pmap)# class c1
switchxxxxxx(config-pmap-c)# mirror 2
switchxxxxxx(config-pmap-c)# exit
switchxxxxxx(config-pmap)# exit
switchxxxxxx(config)#
```

41.14. police

Use the `police` Policy-map Class Configuration mode. command to define the policer for classified traffic. This defines another group of actions for the policy map (per class map). Use the no form of this command to remove a policer.

Syntax

- police committed-rate-kbps committed-burst-byte [exceed-action action] [peak peak-rate-kbps peak-burst-byte [violate-action action]]
- no police

Parameters

- committed-rate-kbps - Specifies the average traffic rate (CIR) in kbits per second (bps).(Range 100–10000000)
- committed-burst-byte - Specifies the normal burst size (CBS) in bytes. (Range: 3000–19173960)
- exceed-action - Specifies the action taken when the committed rate is exceeded and the peak rate is not exceeded. If the keyword is not configured then the following action is applied:
  - drop, if peak the keyword is not configured.
  - policed-dscp-transmit, if peak the keyword is configured.
- peak - Specifies the Two-rate Three-color policer. If the peak rate is exceeded the packet is dropped.
- peak-rate-kbps - Specifies the average traffic rate (CIR) in kbits per second (bps).(Range 100–10000000)
- peak-burst-byte - Specifies the peak burst size (PBS) in bytes. (Range: 3000–19173960)
- violate-action - Specifies the action taken when the peak rate is exceeded. If the keyword is not configured then the drop action is applied.
- action - Specifies the taken action. The possible values are:
  - drop - Drops the packet.
  - policed-dscp-transmit - Remarks the packet DSCP of IP traffic. The DSCP remarking is configured by the qos map policed-dscp command with the violation keyword for the violation action and without this keyword for the exceed action. DSCP remarking will have effect only if the mode is trust dscp.

Default Usage

No policer

Command Mode

Policy-map Class Configuration mode.

User Guidelines

This command is used after the `policy-map` and `class` commands.

This command is only available when QoS is in advanced mode.

Policing uses a token bucket algorithm.

Examples

Example 1. The following example defines a policer for classified traffic. When the traffic rate exceeds 124,000 kbps and the normal burst size exceeds 9600 bytes, the packet is dropped. The class is called class1 and is in a policy map called policy1.

```
switchxxxxxx(config)# policy-map policy1
switchxxxxxx(config-pmap)# class cls1
switchxxxxxx(config-pmap-c)# police 124000 9600 exceed-action drop
```

Example 2. The following example defines a Two-rate Three-color policer for classified traffic. When the committed traffic rate exceeds 124,000 kbps and the committed burst size exceeds 9600 bytes, the packet is marked. When the peak traffic rate exceeds 200,000 kbps and the peak burst size exceeds 19200 bytes, the packet is marked. The class is called class1 and is in a policy map called policy1.

```
switchxxxxxx(config)# policy-map policy1
switchxxxxxx(config-pmap)# class cls1
switchxxxxxx(config-pmap-c)# police 124000 9600 exceed-action policed-dscp-
transmit peak 200000 19200 violate-action policed-dscp-transmit
```

41.15. service-policy

Use the `service-policy` Interface (Ethernet, Port Channel) Configuration mode mode command to bind a policy map to an interface. Use the no form of this command to detach a policy map from an interface.

Syntax

- service-policy {input | output} policy-map-name [default-action {permit-any | deny-any}]
- no service-policy input | output service-policy {input | output} policy-map-name

Parameters

- input - Specifies an ingress policy.
- output - Specifies an egress policy.
- policy-map-name - Specifies the policy map name to apply to the input interface. (Length: 1–32 characters)
- default-action - Specifies the default action. If the keyword is not configured then the deny-any default action is applied.
- deny-any - Deny all the packets (which were ingress of the port) that do not meet the rules in a policy.
- permit-any - Forward all the packets (which were ingress of the port) that do not meet the rules in a policy.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Default

Policy map is not bound.

User Guidelines

This command is only available in QoS advanced mode.

Only one policy map per interface per direction is supported.

If the policy map includes the `police` command a separate copy of the policy map rules is created in TCAM for each Ethernet port.

An egress policy cannot support the following actions:

- `set` with the queue keyword
- trust
- redirect
- mirror
- police

The service-policy output command fails if the bound policy contains actions not supported by egress policies.

A policy map cannot be bound as input and output at the same time.

Example

The following example attaches a policy map called Policy1 to the input interface.

```
switchxxxxxx(config-if)# service-policy input policy1
```

The following example attaches a policy map called Policy1 to the input interface and forwards all packets that do not meet the rules of the policy.

```
switchxxxxxx(config-if)# service-policy input policy1 permit-any
```

The following example attaches a policy map called Policy2 to the output interface.

```
switchxxxxxx(config-if)# service-policy output policy2
```

41.16. qos aggregate-policer

Use the `qos aggregate-policer` Global Configuration mode command to define the policer parameters that can be applied to multiple traffic classes. Use the no form of this command to remove an existing aggregate policer.

Syntax

- qos aggregate-policer aggregate-policer-name committed-rate-kbps committed-burst-byte [exceed-action action] [peak peak-rate-kbps peak-burst-byte [violate-action action]]
- no qos aggregate-policer aggregate-policer-name

Parameters

- aggregate-policer-name - Specifies the aggregate policer name. (Length: 1–32 characters)

- committed-rate-kbps - Specifies the average traffic rate (CIR) in kbits per second (bps).(Range 100–19173960)
- committed-burst-byte - Specifies the normal burst size (CBS) in bytes. (Range: 3000–19173960)
- exceed-action - Specifies the action taken when the committed rate is exceeded and the peak rate is not exceeded. If the keyword is not configured then the following action is applied:
  - drop, if peak the keyword is not configured.
  - policed-dscp-transmit, if peak the keyword is configured.
- peak - Specifies the Two-rate Three-color policer. If the peak rate is exceeded the packet is dropped.
- peak-rate-kbps - Specifies the average traffic rate (CIR) in kbits per second (bps).(Range 100–10000000)
- peak-burst-byte - Specifies the peak burst size (PBS) in bytes. (Range: 3000–19173960)
- violate-action - Specifies the action taken when the peak rate is exceeded. If the keyword is not configured then the drop action is applied.
- action - Specifies the taken action. The possible values are:
  - drop - Drops the packet.
  - policed-dscp-transmit - Remarks the packet DSCP of IP traffic. The DSCP remarking is configured by the qos map policed-dscp command with the violation keyword for the violation action and without this keyword for the exceed action. DSCP remarking will have effect only if the mode is trust dscp.

Default Configuration

No aggregate policer is defined.

Command Mode

Global Configuration mode

User Guidelines

This command is only available when QoS is in advanced mode.

Use the `qos aggregate-policer` command to define a policer that aggregates traffic from multiple class maps.

Aggregate policers cannot aggregate traffic from multiple devices. If the aggregate policer is applied to more than one device, the traffic on each device is counted separately and is limited per device.

Traffic from two different ports on the same device can be aggregated for policing purposes.

An aggregate policer can be applied to multiple classes in the same policy map.

An aggregate policer cannot be deleted if it is being used in a policy map. The no police aggregate Policy-map Class Configuration mode command must first be used to delete the aggregate policer from all policy maps before using the no qos aggregate-policer command.

Policing uses a token bucket algorithm. CIR represents the speed with which the token is added to the bucket. CBS represents the depth of the bucket.

Examples

Example 1. The following example defines the parameters of a policer called policer1 that can be applied to multiple classes in the same policy map. When the average traffic rate exceeds 124,000 kbps or the normal burst size exceeds 9600 bytes, the packet is dropped.

```
switchxxxxxx(config)# qos aggregate-policer policer1 124000 9600 exceed-action
drop
```

Example 2. The following example defines the parameters of a Two-rate Three-color policer called policer2 that can be applied to multiple classes in the same policy map. When the average traffic rate exceeds 124,000 kbps or the normal burst size exceeds 9600 bytes, the packet is remarked. When the average traffic rate exceeds 200,000 kbps or the normal burst size exceeds 9600 bytes, the packet is dropped.

```
switchxxxxxx(config)# qos aggregate-policer policer2 124000 9600 exceed-action
policed-dscp-transmit peak 200000 19200 violate-action policed-dscp-transmit
```

41.17. show qos aggregate-policer

Use the `show qos aggregate-policer` Privileged EXEC mode mode command to display aggregate policers

This command is only available in QoS advanced mode.

Syntax

- show qos aggregate-policer [aggregate-policer-name]

Parameters

- aggregate-policer-name - Specifies the aggregate policer name. (Length: 1–32 characters)

Default Configuration

All policers are displayed.

Command Mode

Privileged EXEC mode

Examples

Example 1. The following example displays the parameters of the aggregate policer called Policer1.

```
switchxxxxxx# show qos aggregate-policer policer1 aggregate-policer policer1
96000 4800 exceed-action drop not used by any policy map.
```

Example 2. The following example displays the parameters of the aggregate Two-rate Three-color policer called Policer1.

```
switchxxxxxx# show qos aggregate-policer policer1
aggregate-policer policer1 124000 9600 exceed-action policed-dscp-transmit peak
200000 19200 violate-action policed-dscp-transmit not used by any policy map.
```

41.18. police aggregate

Use the `police aggregate` Policy-map Class Configuration mode. command to apply an aggregate policer to multiple class maps within the same policy map. Use the no form of this command to remove an existing aggregate policer from a policy map.

This command is only available in QoS advanced mode.

Syntax

- police aggregate aggregate-policer-name
- no police aggregate aggregate-policer-name

Parameters

- aggregate-policer-name - Specifies the aggregate policer name. (Length: 1–32 characters)

Command Mode

Policy-map Class Configuration mode.

User Guidelines

An aggregate policer can be applied to multiple classes in the same policy map.

An aggregate policer cannot be applied across multiple policy maps or interfaces.

Use the `exit` command to return to the Configuration mode. Use the `end` command to return to the Privileged EXEC mode.

Example

The following example applies the aggregate policer called Policer1 to a class called class1 in a policy map called policy1 and class2 in policy map policy2.

```
switchxxxxxx(config)# qos aggregate-policer
policer1 124000 9600 exceed-action drop
switchxxxxxx(config)# policy-map policy1
switchxxxxxx(config-pmap)# class class1
switchxxxxxx(config-pmap-c)# police aggregate policer1
switchxxxxxx(config-pmap-c)# exit
switchxxxxxx(config-pmap)# exit
switchxxxxxx(config)# policy-map policy2
switchxxxxxx(config-pmap)# class class2
switchxxxxxx(config-pmap-c)# police aggregate policer1
```

41.19. wrr-queue cos-map

Use the `wrr-queue cos-map` Global Configuration mode command to map Class of Service (CoS) values to a specific egress queue. Use the no form of this command to restore the default configuration.

Syntax

- wrr-queue cos-map queue-id cos0... cos7
- no wrr-queue cos-map [queue-id]

Parameters

- queue-id - Specifies the queue number to which the CoS values are mapped.

- cos0... cos7 - Specifies up to 8 CoS values to map to the specified queue number. (Range: 1–254)

Default Configuration

The default CoS value mapping to 8 queues is as follows:

- CoS value 1 is mapped to queue 1.
- CoS value 2 is mapped to queue 2.
- CoS value 8 is mapped to queue 3.
- CoS value 16 is mapped to queue 4.
- CoS value 32 is mapped to queue 5.
- CoS value 64 is mapped to queue 6.
- CoS value 128 is mapped to queue 7.
- CoS value 254 is mapped to queue 8.

Command Mode

Global Configuration mode

User Guidelines

Use this command to distribute traffic to different queues.

Example

The following example maps CoS value 4 and 6 to queue 2.

```
switchxxxxxx(config)# wrr-queue cos-map 2 4 6
```

41.20. wrr-queue bandwidth

Use the `wrr-queue bandwidth` Global Configuration mode command to assign Weighted Round Robin (WRR) weights to egress queues. The weight ratio determines the frequency at which the packet scheduler removes packets from each queue. Use the no form of this command to restore the default configuration.

Syntax

- wrr-queue bandwidth weight1 weight2... weighting
- no wrr-queue bandwidth

Parameters

- weight1 weight1... weighting the ratio of bandwidth assigned by the WRR packet scheduler to the packet queues. See explanation in the User Guidelines. Separate each value by a space. (Range for each weight: 0–255)

Default Configuration

wrr is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

The ratio for each queue is defined as the queue weight divided by the sum of all queue weights (the normalized weight). This sets the bandwidth allocation of each queue.

A weight of 0 indicates that no bandwidth is allocated for the same queue, and the shared bandwidth is divided among the remaining queues. It is not recommended

to set the weight of a queue to a 0 as it might stop transmission of control-protocols packets generated by the device.

All queues participate in the WRR, excluding the expedite queues, whose corresponding weight is not used in the ratio calculation.

An expedite queue is a priority queue, which is serviced until empty before the other queues are serviced. The expedite queues are designated by the `priority-queue out num-of-queues` command.

Example

The following assigns WRR values to the queues.

```
switchxxxxxx(config)# priority-queue out num-of-queues 0
switchxxxxxx(config)# wrr-queue bandwidth 6 6 6 6 6 6 6 6
```

41.21. priority-queue out num-of-queues

Use the `priority-queue out num-of-queues` Global Configuration mode command to configure the number of expedite queues. Use the no form of this command to restore the default configuration.

Syntax

- priority-queue out num-of-queues number-of-queues
- no priority-queue out num-of-queues

Parameters

- number-of-queues - Specifies the number of expedite (strict priority) queues. Expedite queues are assigned to the queues with the higher indexes. (Range: 0–8 .There must be either 0 wrr queues or more than one.

If number-of-queues = 0, all queues are assured forwarding (according to wrr weights) If the number-of-queues = 8 , all the queues are expedited (strict priority queues).

Default Configuration

All queues are expedite queues.

Command Mode

Global Configuration mode

User Guidelines

An expedite queue is a strict priority queue, which is serviced until empty before the other lower priority queues are serviced.

the weighted round robin (WRR) weight ratios are affected by the number of expedited queues, because there are fewer queues participating in WRR. This indicates that the corresponding weight in the wrr-queue bandwidth Interface Configuration mode command is ignored (not used in the ratio calculation).

Example

The following example configures the number of expedite queues as 2.

```
switchxxxxxx(config)# priority-queue out num-of-queues 2
```

41.22. traffic-shape

Use the `traffic-shape` Interface (Ethernet, Port Channel) Configuration mode command to configure the egress port shaper. Use the no form of this command to disable the shaper.

Syntax

- traffic-shape committed-rate [committed-burst]
- no traffic-shape

Parameters

- committed-rate - Specifies the maximum average traffic rate (CIR) in kbits per second (kbps). (Range: ,10GE: 64Kbps–maximum port speed))
- committed-burst - Specifies the maximum permitted excess burst size

(CBS) in bytes. (Range: 4096 - 16762902 bytes)

Default Configuration

The shaper is disabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The egress port shaper controls the traffic transmit rate (Tx rate) on a port.

Example

The following example sets a traffic shaper on te1/0/1 when the average traffic rate exceeds 64 kbps or the normal burst size exceeds 4096 bytes.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# traffic-shape 64 4096
```

41.23. traffic-shape queue

Use the `traffic-shape queue` Interface (Ethernet, Port Channel) Configuration mode command to configure the egress queue shaper. Use the no form of this command to disable the shaper.

Syntax

- traffic-shape queue queue-id committed-rate [committed-burst]
- no traffic-shape queue queue-id

Parameters

- queue-id - Specifies the queue number to which the shaper is assigned. (Range: 1-8).
- committed-rate - Specifies the average traffic rate (CIR) in kbits per second (kbps). (Range: 64 kbps–maximum port speed)
- committed-burst - Specifies the excess burst size (CBS) in bytes. (Range: 4096 - 16762902 bytes)

Default Configuration

The shaper is disabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The egress port shaper controls the traffic transmit rate (Tx rate) on a queue on a port.

Example

The following example sets a shaper on queue 1 on te1/0/1 when the average traffic rate exceeds 124000 kbps or the normal burst size exceeds 9600 bytes.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# traffic-shape queue 1 64 4096
```

41.24. show qos interface

Use the `show qos interface` Privileged EXEC mode command to display Quality of Service (QoS) information on the interface.

Syntax

- show qos interface [buffers | queueing | policers | shapers] [interface-id]

Parameters

- buffers - Displays the buffer settings for the interface's queues. For GE ports, displays the queue depth for each of the queues.
- queueing - Displays the queue's strategy (WRR or EF), the weight for WRR queues, the CoS to queue map and the EF priority.
- policers - Displays all the policers configured for this interface, their settings, and the number of policers currently unused (on a VLAN).
- shapers - Displays the shaper of the specified interface and the shaper for the queue on the specified interface.
- interface-id - Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, or Port-channel.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

If no parameter is specified with the show qos interface command, the port QoS mode (DSCP trusted, CoS trusted, untrusted, and so on), default CoS value, DSCP-to-DSCP- map (if any) attached to the port, and policy map (if any) attached to the interface are displayed. If a specific interface is not specified, the information for all interfaces is displayed.

In case of Policers, Shapers and Rate Limit - only the ports which are not in the default configuration will be showed.

Examples

Example 1 - The following is an example of the output from the show qos interface command.

```
switchxxxxxx(config)# show qos interface te1/0/1
Ethernet te1/0/0/1
Default CoS: 0
Trust mode: disabled
Ingress Policy applied: AV1
Egress Policy applied: AV2
```

```
Default ACE ingress action: deny-all
Default ACE egress action: deny-all
```

Example 2 - The following is an example of the output from the show qos interface queueing command for 4 queues.

```
switchxxxxxx(config)# show qos interface queueing
te1/0/1 Ethernet te1/0/0/1 wrr bandwidth weights and EF priority:
qid-weights Ef - Priority
- N/A ena- 1
- N/A ena- 2
- N/A ena- 3
- N/A ena- 4
Cos-queue map:
cos-qid 0 - 1
- 1
- 2
- 3
- 3
- 4
- 4
- 4
```

Example 3 - The following an example of the output from the show qos interface buffers command for 8 queues

```
switchxxxxxx(config)# show qos interface buffers te1/0/1 te1/0/1
Notify Q depth: buffers te1/0/1 Ethernet te1/0/1 qid thresh0 thresh1 thresh2 1
100 100 80
100 100 80
100 100 80
100 100 80
100 100 80
100 100 80
100 100 80
100 100 80
```

Example 4 - This is an example of the output from the show qos interface shapers command.

```
switchxxxxxx(config)# show qos interface shapers te1/0/1
te1/0/1
Port shaper: enable
Committed rate: 64 kbps
Committed burst: 9600 bytes
 Target Target
QID Status Committed Committed
 Rate [kbps] Burst [bytes]
1 Enable 64 17000
2 Disable N/A N/A
3 Enable N/A N/A
4 Disable N/A N/A
5 Disable N/A N/A
6 Disable N/A N/A
7 Enable N/A N/A
8 Enable N/A N/A
```

Example 5 - This is an example of the output from show qos interface policer

```
switchxxxxxx(config)# show qos interface policer te1/0/1
Ethernet te1/0/1
Ingress Policers:
Class map: A
Policer type: aggregate
Commited rate: 19 kbps
Commited burst: 9600 bytes
Exceed-action: policed-dscp-transmit
Class map: B
Policer type: single
Commited rate: 19 kbps
Commited burst: 9600 bytes
Peak rate: 26 kbps
Peak burst: 9600 bytes
Exceed-action: policed-dscp-transmit
Violate-action: drop
Class map: C Policer type: none Egress Policers:
Class map: D
```

41.25. qos map policed-dscp

Use the `qos map policed-dscp` Global Configuration mode command to configure the policed-DSCP map for remarking purposes. Use the no form of this command to restore the default configuration.

Syntax

- qos map policed-dscp [violation] dscp-list to dscp-mark-down
- no qos map policed-dscp [violation] [dscp-list]

Parameters

- violation - Specifies the DSCP remapping in the violate action. If the keyword is not configured the the command specifies the DSCP remapping in the exceed action.
- dscp-list - Specifies up to 8 DSCP values, separated by spaces. (Range: 0– 63)
- dscp-mark-down - Specifies the DSCP value to mark down. (Range: 0–63)

Default Configuration

The default map is the Null map, which means that each incoming DSCP value is mapped to the same DSCP value.

Command Mode

Global Configuration mode

User Guidelines

The original DSCP value and policed-DSCP value must be mapped to the same queue in order to prevent reordering.

Example

The following example marks incoming DSCP value 3 as DSCP value 5 on the policed-DSCP map.

```
switchxxxxxx(config)# qos map policed-dscp 3 to 5
```

41.26. qos map dscp-queue

Use the `qos map dscp-queue` Global Configuration mode command to configure the DSCP to queue map. Use the no form of this command to restore the default configuration.

Syntax

- qos map dscp-queue dscp-list to queue-id
- no qos map dscp-queue [dscp-list]

Parameters

- dscp-list - Specifies up to 8 DSCP values, separated by spaces. (Range: 0– 63)
- queue-id - Specifies the queue number to which the DSCP values are mapped.

Default Configuration

The default map for 8 queues is as follows.

DSCP value	0	1-8	9-15	16,24,40,48-63	17-23	25-31	33-39	32,41-47
Queue-ID	2	1	3	7	4	5	6	8

Command Mode

Global Configuration mode

Example

The following example maps DSCP values 33, 40 and 41 to queue 1.

```
switchxxxxxx(config)# qos map dscp-queue 33 40 41 to 1
```

41.27. qos trust (Global)

Use the `qos trust` Global Configuration mode command to configure the system to the basic mode and trust state. Use the no form of this command to return to the default configuration.

Syntax

- qos trust {cos | dscp}
- no qos trust

Parameters

- cos - Specifies that ingress packets are classified with packet CoS values. Untagged packets are classified with the default port CoS value.
- dscp - Specifies that ingress packets are classified with packet DSCP values.

Default Configuration

dscp

Command Mode

Global Configuration mode

User Guidelines

This command can be used only in QoS basic mode.

Packets entering a QoS domain are classified at its edge. When the packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every switch within the domain.

Use this command to specify whether the port is trusted and which fields of the packet to use to classify traffic.

When the system is configured with trust DSCP, the traffic is mapped to the queue by the DSCP-queue map.

When the system is configured with trust CoS, the traffic is mapped to the queue by the CoS-queue map.

For an inter-QoS domain boundary, configure the port to the DSCP-trusted state and apply the DSCP-to-DSCP-mutation map if the DSCP values are different in the QoS domains.

Example

The following example configures the system to the DSCP trust state.

```
switchxxxxxx(config)# qos trust dscp
```

41.28. qos trust (Interface)

Use the `qos trust` Interface (Ethernet, Port Channel) Configuration mode command to enable port trust state while the system is in the basic QoS mode. Use the no form of this command to disable the trust state on each port.

Syntax

- qos trust
- no qos trust

Parameters

N/A

Default Configuration

Each port is enabled while the system is in basic mode.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example configures te1/0/1 to the default trust state.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# qos trust
```

41.29. qos cos

Use the `qos cos` Interface (Ethernet, Port Channel) Configuration mode command to define the default CoS value of a port. Use the no form of this command to restore the default configuration.

Syntax

- qos cos default-cos
- no qos cos

Parameters

- default-cos - Specifies the default CoS value (VPT value) of the port. If the port is trusted and the packet is untagged, then the default CoS value become the CoS value. (Range: 0–7)

Default Configuration

The default CoS value of a port is 0.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use the default CoS value to assign a CoS value to all untagged packets entering the interface.

Example

The following example defines the port `te1/0/1` default CoS value as 3.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# qos cos 3
```

41.30. qos dscp-mutation

Use the `qos dscp-mutation` Global Configuration mode command to apply the DSCP Mutation map to system DSCP trusted ports. Use the no form of this command to restore the trusted port with no DSCP mutation.

Syntax

- qos dscp-mutation
- no qos dscp-mutation

Parameters

N/A

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

Apply the DSCP-to-DSCP-mutation map to a port at the boundary of a Quality of

Service (QoS) administrative domain. If two QoS domains have different DSCP definitions, use the DSCP-to-DSCP-mutation map to translate a set of DSCP values to match the definition of another domain. Apply the map to ingress and to DSCP-trusted ports only. Applying this map to a port causes IP packets to be rewritten with newly mapped DSCP values at the ingress ports. If applying the DSCP mutation map to an untrusted port, to class of service (CoS), or to an IP-precedence trusted port.

Global trust mode must be DSCP or CoS-DSCP. In advanced CoS mode, ports must be trusted.

Example

The following example applies the DSCP Mutation map to system DSCP trusted ports.

```
switchxxxxxx(config)# qos dscp-mutation
```

41.31. qos map dscp-mutation

Use the `qos map dscp-mutation` Global Configuration modecommand to configure the DSCP to DSCP Mutation table. Use the no form of this command to restore the default configuration.

Syntax

- qos map dscp-mutation in-dscp to out-dscp
- no qos map dscp-mutation [in-dscp]

Parameters

- in-dscp - Specifies up to 8 DSCP values to map, separated by spaces. (Range: 0–63)
- out-dscp - Specifies up to 8 DSCP mapped values, separated by spaces. (Range: 0–63)

Default Configuration

The default map is the Null map, which means that each incoming DSCP value is mapped to the same DSCP value.

Command Mode

Global Configuration mode

User Guidelines

This is the only map that is not globally configured. It is possible to have several maps and assign each one to a different port.

Example

The following example changes DSCP values 1, 2, 4, 5 and 6 to DSCP Mutation Map value 63.

```
switchxxxxxx(config)# qos map dscp-mutation 1 2 4 5 6 to 63
```

41.32. show qos map

Use the `show qos map` Privileged EXEC mode command to display the various types of QoS mapping.

Syntax

- show qos map [dscp-queue | dscp-dp | policed-dscp | dscp-mutation]

Parameters

- dscp-queue - Displays the DSCP to queue map.
- dscp-dp - Displays the DSCP to Drop Precedence map.
- policed-dscp - Displays the DSCP to DSCP remark table.
- dscp-mutation - Displays the DSCP-DSCP mutation table.

Default Configuration

Display all maps.

Command Mode

Privileged EXEC mode

Examples

Example 1. The following example displays the QoS mapping information:

```
switchxxxxxx(config)# show qos map dscp-queue
Dscp-queue map:
 d1 : d2 0 1 2 3 4 5 6 7 8 9
 ----------------------------------
: 01 01 01 01 01 01 01 01 01 01
: 01 01 01 01 01 01 02 02 02 02
: 02 02 02 02 02 02 02 02 02 02
: 02 02 03 03 03 03 03 03 03 03
: 03 03 03 03 03 03 03 03 04 04 5
: 04 04 04 04 04 04 04 04 04 04
 6 : 04 04 04 04
```

Example 2. The following example displays the dscp remapping information:

```
switchxxxxxx(config)# show qos map policed-dscp
Policed-dscp map (exceed):
 d1 : d2 0 1 2 3 4 5 6 7 8 9
 ----------------------------------
: 00 01 02 03 04 05 06 07 08 09
: 10 11 12 13 14 15 16 17 18 19
: 20 21 22 23 24 25 26 27 28 29
: 30 31 32 33 34 35 36 37 38 39
: 40 41 42 43 44 45 46 47 48 49
5 : 50 51 52 53 54 55 56 57 58 59
6 : 21 21 21 Policed-dscp map (violate):
 d1 : d2 0 1 2 3 4 5 6 7 8 9
 ----------------------------------
0 : 00 01 02 03 04 05 06 07 08 09
: 10 11 12 13 14 15 16 17 18 19
: 20 21 22 23 24 25 26 27 28 29
: 30 31 32 33 34 35 36 37 38 39
: 40 41 42 43 44 45 46 47 48 49
5 : 50 51 52 53 54 55 56 57 58 59
 6 : 11 11 11
```

41.33. clear qos statistics

Use the `clear qos statistics` Privileged EXEC mode command to clear the QoS statistics counters.

Syntax

- clear qos statistics

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example clears the QoS statistics counters.

```
switchxxxxxx(config)# clear qos statistics
```

41.34. qos statistics policer

Use the `qos statistics policer` Interface (Ethernet, Port Channel) Configuration mode mode command to enable counting in-profile and out-of-profile. Use the no form of this command to disable counting.

This command is relevant only when policers are defined.

Syntax

- qos statistics policer policy-map-name class-map-name
- no qos statistics policer policy-map-name class-map-name

Parameters

- policy-map-name - Specifies the policy map name. (Length: 1–32 characters)
- class-map-name - Specifies the class map name. (Length: 1–32 characters)

Default Configuration

Counting in-profile and out-of-profile is disabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example enables counting in-profile and out-of-profile on the interface.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# qos statistics policer policy1 class1
```

41.35. qos statistics aggregate-policer

Use the `qos statistics aggregate-policer` Global Configuration mode command to enable counting in-profile and out-of-profile. Use the no form of this command to disable counting.

Syntax

- qos statistics aggregate-policer aggregate-policer-name
- no qos statistics aggregate-policer aggregate-policer-name

Parameters

- aggregate-policer-name - Specifies the aggregate policer name. (Length: 1–32 characters)

Default Configuration

Counting in-profile and out-of-profile is disabled.

Command Mode

Global Configuration mode

Example

The following example enables counting in-profile and out-of-profile on the interface.

```
switchxxxxxx(config)# qos statistics aggregate-policer policer1
```

41.36. qos statistics queues

Use the `qos statistics queues` Global Configuration mode command to enable QoS statistics for output queues. Use the no form of this command to disable QoS statistics for output queues.

Syntax

- qos statistics queues set {queue | all} {dp | all} {interface | all}
- no qos statistics queues set

Parameters

- set - Specifies the counter set number.
- interface - Specifies the Ethernet port.
- queue - Specifies the output queue number (up to 8 queues).
- dp - Specifies the drop precedence. The available values are: high, low.

Default Configuration

Set 1: All interfaces, all queues, high DP.

Set 2: All interfaces, all queues, low DP.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

If the queue parameter is all, traffic in cascading ports is also counted.

Example

The following example enables QoS statistics for output queues for counter set 1.

```
switchxxxxxx(config)# qos statistics queues 1 all all all
```

41.37. show qos statistics

Use the `show qos statistics` Privileged EXEC mode command to display Quality of Service statistical information.

Syntax

- show qos statistics

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

Use the `show qos statistics` command to display QoS statistics.

Up to 16 sets of counters can be enabled for policers. The counters can be enabled in the creation of the policers.

Use the `qos statistics queues` Global Configuration mode command to enable QoS statistics for output queues.

Example

The following example displays Quality of Service statistical information.

```
switchxxxxxx# show qos statistics
Policers
---------
Interface Policy Class In-Profile Peak Violate
 Map Map Bytes Bytes Bytes
--------- ------ ----- ---------- ----- -------
te1/0/1 Policy1 Class1 756457 5427 12
te1/0/1 Policy1 Class2 8759 14 12
te1/0/2 Policy1 Class1 75457 2
te1/0/2 Policy1 Class2 5326 5 12

Aggregate Policers
------------------
Name In-Profile Peak Violate
 Bytes Bytes Bytes
---- ---------- ----- -------
Policer 756457 5427 12

Output Queues
-------------
Interface Queue DP Total TD
 Packets Packets
--------- ----- -- ------- -------
te1/0/1 2 High 756457 1.2%
te1/0/2 All High 8759 0.2%
```

42. RADIUS Commands

42.1. radius-server host

Use the `radius-server host` Global Configuration mode command to configure up to 8 RADIUS server hosts supporting the DVA attribute. Use the no form of the command to delete the specified RADIUS server host.

Syntax

- radius-server host {ip-address | hostname} [auth-port auth-port-number] [acct-port acct-port-number] [timeout timeout] [retransmit retries] [deadtime deadtime] [key key-string] [priority priority] [usage {login | dot1.x | all}]
- no radius-server host {ip-address | hostname}

Parameters

- ip-address - Specifies the RADIUS server host IP address. The IP address can be an IPv4, IPv6 or IPv6 address.
- hostname - Specifies the RADIUS server host name. Translation to IPv4 addresses only is supported. (Length: 1–158 characters. Maximum label length of each part of the hostname: 63 characters)
- auth-port auth-port-number - Specifies the port number for authentication requests. If the port number is set to 0, the host is not used for authentication. (Range: 0–65535)
- acct-port acct-port-number - Port number for accounting requests. The host is not used for accountings if set to 0. If unspecified, the port number defaults to 1813.
- timeout timeout - Specifies the timeout value in seconds. (Range: 1–30)
- retransmit retries - Specifies the number of retry retransmissions (Range: 1–15)
- deadtime deadtime - Specifies the length of time in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0–2000)
- key key-string - Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. To specify an empty string, enter "". (Length: 0–128 characters). If this parameter is omitted, the globally-configured radius key will be used.
- priority priority - Specifies the order in which servers are used, where 0 has the highest priority. (Range: 0–65535)
- usage {login | dot1.x | all} - Specifies the RADIUS server usage type. The possible values are:
  - login - Specifies that the RADIUS server is used for user login parameters authentication.
  - dot1.x - Specifies that the RADIUS server is used for 802.1x port authentication.
  - all - Specifies that the RADIUS server is used for user login authentication and 802.1x port authentication.

Default Configuration

The default authentication port number is 1812.

If timeout is not specified, the global value (set in the `radius-server timeout` command) is used.

If retransmit is not specified, the global value (set in the `radius-server retransmit` command) is used.

If key-string is not specified, the global value (set in the `radius-server key` command) is used.

If the usage keyword is not specified, the all argument is applied.

Command Mode

Global Configuration mode

User Guidelines

To specify multiple hosts, this command is used for each host.

Example

The following example specifies a RADIUS server host with IP address 192.168.10.1, authentication request port number 20, and a 20-second timeout period.

```
switchxxxxxx(config)# radius-server host 192.168.10.1 auth-port 20 timeout 20
```

42.2. radius-server key

Use the `radius-server key` Global Configuration mode command to set the authentication key for RADIUS communications between the device and the RADIUS daemon. Use the no form of this command to restore the default configuration.

Syntax

- radius-server key [key-string]
- no radius-server key

Parameters

- key-string - Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. (Range: 0–128 characters)

Default Configuration

The key-string is an empty string.

Command Mode

Global Configuration mode

Example

The following example defines the authentication key for all RADIUS communications between the device and the RADIUS daemon.

```
switchxxxxxx(config)# radius-server key enterprise-server
```

42.3. radius-server retransmit

Use the `radius-server retransmit` Global Configuration mode command to specify the number of times the software searches the list of RADIUS server hosts. Use the no form of this command to restore the default configuration.

Syntax

- radius-server retransmit retries
- no radius-server retransmit

Parameters

- retransmit retries - Specifies the number of retry retransmissions (Range: 1–15).

Default Configuration

The software searches the list of RADIUS server hosts 3 times.

Command Mode

Global Configuration mode

Example

The following example configures the number of times the software searches all RADIUS server hosts as 5.

```
switchxxxxxx(config)# radius-server retransmit 5
```

42.4. radius-server host source-interface

Use the `radius-server host source-interface` Global Configuration mode command to specify the source interface whose IPv4 address will be used as the Source IPv4 address for communication with IPv4 RADIUS servers. Use the no form of this command to restore the default configuration.

Syntax

- radius-server host source-interface interface-id
- no radius-server host source-interface

Parameters

- interface-id - Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the interface IP address belonging to next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface, the minimal IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 RADIUS server.

OOB cannot be defined as a source interface.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# radius-server host source-interface vlan 100
```

42.5. radius-server host source-interface-ipv6

Use the `radius-server host source-interface-ipv6` Global Configuration mode command to specify the source interface whose IPv6 address will be used as the source IPv6 address for communication with IPv6 RADIUS servers. Use the no form of this command to restore the default configuration.

Syntax

- radius-server host source-interface-ipv6 interface-id
- no radius-server host source-interface-ipv6

Parameters

- interface-id - Specifies the source interface.

Default Configuration

The IPv6 source address is the IPv6 address defined on the outgoing interface and selected in accordance with RFC6724.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the source IPv6 address is an IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

If the source interface is not the outgoing interface, the source IPv6 address is the minimal IPv6 address defined on the source interface and matched to the scope of the destination IPv6 address is applied.

If there is no available source IPv6 address, a SYSLOG message is issued when attempting to communicate with an IPv6 RADIUS server.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# radius-server host source-interface-ipv6 vlan 100
```

42.6. radius-server timeout

Use the `radius-server timeout` Global Configuration mode command to set how long the device waits for a server host to reply. Use the no form of this command to restore the default configuration.

Syntax

- radius-server timeout timeout-seconds
- no radius-server timeout

Parameters

- timeout timeout-seconds - Specifies the timeout value in seconds. (Range: 1–30).

Default Configuration

The default timeout value is 3 seconds.

Command Mode

Global Configuration mode

Example

The following example sets the timeout interval on all RADIUS servers to 5 seconds.

```
switchxxxxxx(config)# radius-server timeout 5
```

42.7. radius-server deadtime

Use the `radius-server deadtime` Global Configuration mode command to configure how long unavailable RADIUS servers are skipped over by transaction requests. This improves RADIUS response time when servers are unavailable. Use the no form of this command to restore the default configuration.

Syntax

- radius-server deadtime deadtime
- no radius-server deadtime

Parameters

- deadtime - Specifies the time interval in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0–2000).

Default Configuration

The default deadtime interval is 0.

Command Mode

Global Configuration mode

Example

The following example sets all RADIUS server deadtimes to 10 minutes.

```
switchxxxxxx(config)# radius-server deadtime 10
```

42.8. show radius-servers

Use the `show radius-servers` Privileged EXEC mode command to display the RADIUS server settings.

Syntax

- show radius-servers

Command Mode

Privileged EXEC mode

Example

The following example displays RADIUS server settings:

```
switchxxxxxx# show radius-servers
IP address Port Port Time Dead
 Auth Acc Out Retransmision time Priority Usage
---------- ---- ---- ---- ------------ ------ -------- -----
172.16.1.1 1812 1813 125 Global Global 1 All
172.16.1.2 1812 1813 102 8 Global 2 All
```

```
Global values
--------------
TimeOut: 3
Retransmit: 3
Deadtime: 0
Source IPv4 interface: vlan 120 Source IPv6 interface: vlan 10
```

42.9. show radius-servers key

Use the `show radius-servers key` Privileged EXEC mode command to display the RADIUS server key settings.

Syntax

- show radius-servers key

Command Mode

Privileged EXEC mode

Example

The following example displays RADIUS server key settings

```
switchxxxxxx# show radius-servers key
IP address Key
---------- ---
172.16.1.1 Sharon123
172.16.1.2 Bruce123

Global key
--------------
Alice456
```

43. Rate Limit and Storm Control Commands

43.1. clear storm-control counters

To clear storm control counters, use the `clear storm-control counters` command in Privileged EXEC mode.

Syntax

- clear storm-control counters [broadcast | multicast | unicast] [interface interface-id]

Parameters

- broadcast - (Optional) Clear Broadcast storm control counters.
- multicast - (Optional) Clear Multicast storm control counters.
- unicast - (Optional) Clear Unicast Unknown storm control counters.
- interface interface-id - (Optional) Clear storm control counters for the specified Ethernet port.

Command Mode

Privileged EXEC mode

User Guidelines

The switch clears the port counter of a given traffic type when storm control for this traffic type on this port is enabled.

Use this command to clear the storm control counters when storm control is running.

Use the `clear storm-control counters` command to clear all the storm control counters of all Ethernet ports.

Use the `clear storm-control counters interface interface-id` command to clear all the storm control counters of a given port.

Use the clear storm-control counters broadcast | multicast | unicast command to clear all storm control counters of a given traffic type of all Ethernet ports.

Use the clear storm-control counters broadcast | multicast | unicast interface interface-id command to clear one storm control counter of a given traffic type and

of a given port.

Example

Example 1. The following example clears all storm control counters of all ports:

```
switchxxxxxx# clear storm-control counters
```

Example 2. The following example clears all storm control counters of port te1/0/1:

```
switchxxxxxx# clear storm-control counters interface te1/0/1
```

Example 3. The following example clears broadcast storm control counter of all ports:

```
switchxxxxxx# clear storm-control counters broascat
```

Example 4. The following example clears multicast storm control counter of port te1/0/1:

```
switchxxxxxx# clear storm-control counters multicast interface te1/0/1
```

43.2. rate-limit (Ethernet)

To limit the incoming traffic rate on a port, use the `rate-limit` command in Interface (Ethernet) Configuration mode. To disable the rate limit, use the no form of this command.

Syntax

- rate-limit committed-rate-kbps [burst committed-burst-bytes]
- no rate-limit

Parameters

- committed-rate-kbps - Specifies the maximum number of kilobits per second of ingress traffic on a port. The range is 3–maximal port speed.
- burst committed-burst-bytes - (Optional) The burst size in bytes. (Range: 3000–19173960). If unspecified, defaults to 128K.

Default Configuration

Rate limiting is disabled.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

The calculated rate includes the 20 bytes of Ethernet framing overhead (preamble+SFD+IPG).

The Rate Limit does not calculate traffic controlled by Storm control. The real allowed rate will be sum of the rate specified by the command and the rates specified by the Storm control commands for particular traffic types.

Example

The following example limits the incoming traffic rate on te1/0/1 to 150,000 kbps.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# rate-limit 150000
```

43.3. rate-limit vlan

To limit the incoming traffic rate for a VLAN in, use the `rate-limit vlan` command in Global Configuration mode. To disable the rate limit, use the no form of this command.

Syntax

- rate-limit vlan vlan-id committed-rate [burst committed-burst-bytes]
- no rate-limit vlan vlan-id

Parameters

- vlan-id - Specifies the VLAN ID.
- committed-rate - Specifies the average traffic rate (CIR) in kbits per second (kbps). (Range: 3-57982058)
- burst committed-burst - (Optional) Specifies the maximum burst size (CBS) in bytes. (Range: 3000–19173960). If unspecified, defaults to 128K.

Default Configuration

Rate limiting is disabled.

Command Mode

Global Configuration mode

User Guidelines

The calculated rate includes the 20 bytes of Ethernet framing overhead (preamble+SFD+IPG).

Traffic policing in a policy map takes precedence over VLAN rate limiting. If a packet is subject to traffic policing in a policy map and is associated with a VLAN that is rate limited, the packet is counted only in the traffic policing of the policy map.

It does not work in conjunction with IP Source Guard.

Example

The following example limits the rate on VLAN 11 to 150000 kbps or the normal burst size to 9600 bytes.

```
switchxxxxxx(config)# rate-limit vlan 11 150000 burst 9600
```

43.4. storm-control

To enable broadcast, multicast, or unicast storm control on a port, use the `storm-control` command in Interface (Ethernet) Configuration mode. To return to default, use the no form of this command.

Syntax

- storm-control broadcast {level level | kbps kbps} [trap] [shutdown]
- no storm-control broadcast
- storm-control multicast [registered | unregistered] {level level | kbps kbps} [trap] [shutdown]
- no storm-control multicast
- storm-control unicast {level level | kbps kbps} [trap] [shutdown]
- no storm-control unicast no storm-control

Parameters

- broadcast - Enables broadcast storm control on the port.
- multicast [registered | unregistered] - Enables ether all multicast, only registered multicast, or only unregistered multicast storm control on the port.
- unicast - Enables unicast unknown storm control on the port.
- level level - Suppression level in percentage. Block the flooding of storm packets when the value specified for level is reached. (Range 1-100)
- kbps kbps - Maximum of kilobits per second of Broadcast traffic on a port. (Range 1 – 10000000)
- trap - (Optional) Sends a trap when a storm occurs on a port. If the keyword is not specified the trap is not sent.
- shutdown - (Optional) Shut down a port when a storm occurs on the port. If the keyword is not specified extra traffic is discarded.

Default Configuration

Storm control is disabled.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

The calculated rate includes the 20 bytes of Ethernet framing overhead (preamble+SFD+IPG).

The rate limit on a port does not calculate traffic controlled by storm control on this port.

Use the no storm-control command to disable storm control of all traffic type on the port.

You can use the following commands to reset an interface shut down by Storm Control:

- The `errdisable recovery reset` command with the interface interface-id parameter to reset a given interface.
- The `errdisable recovery cause` with the storm-control parameter to automatically recover from the Storm Control error-disabled state.

Example

The following example enables broadcast, multicast, and unicast unknown storm control on port te1/0/1 and multicast unregistered and unicast unknown on port te1/0/2:

Enable group 1 for registered and unregistered multicast traffic on interface te1/0/1. Extra traffic is discarded.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# storm-control broadcast kbps 10000 shutdown
switchxxxxxx(config-if)# storm-control multicast level 20 trap
switchxxxxxx(config-if)# storm-control unicast level 5 trap shutdown
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# interface te1/0/2
switchxxxxxx(config-if)# storm-control multicast unregistered level 5 trap
shutdown
switchxxxxxx(config-if)# storm-control unicast level 5 trap
switchxxxxxx(config-if)# exit
```

43.5. show rate-limit interface

To display rate limit configuration on an interface, use the `show rate-limit interface` command in Privileged EXEC mode.

Syntax

- show rate-limit interface [interface-id]

Parameters

- interface-id - (Optional) Specifies an Ethernet port. If the argument is not configured rate limit configuration of all Ethernet ports is displayed.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Examples

The following is an example of the output from the show rate-limit interface:

```
switchxxxxxx> show rate-limit interface
      Interface   Rate Limit (kbps) Burst (Bytes)
      ------------      ----------------------  ----------------
```

```
      -     -
te1/0/1te1/0/
      2     80000 512
      100000      1024
```

43.6. show rate-limit vlan

To display rate limit configuration on a VLAN, use the `show rate-limit vlan` command in Privileged EXEC mode.

Syntax

- show rate-limit vlan [vlan-id]

Parameters

- vlan-id - (Optional) Specifies a VLAN ID If the argument is not configured rate limit configuration of all VLANs is displayed.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Examples

The following is an example of the output from the show rate-limit vlan:

```
switchxxxxxx> show rate-limit vlan 1075
VLAN Rate Limit (kbps) Burst (Bytes)
---- ----------------- -------------
1075 100000 1024
```

43.7. show storm-control interface

To display storm control information of an interface, use the `show storm-control interface` command in Privileged EXEC mode.

Syntax

- show storm-control interface [interface-id]

Parameters

- interface-id - (Optional) Specifies an Ethernet port. If the argument is not configured storm control information of all Ethernet ports is displayed.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Examples

The following is an example of the output from the show storm-control interface:

```
switchxxxxxx> show storm-control interface
te1/0/1
```

```
Broadacst
Rate: 5%
Action: Shutdown
Passed Counter (Bytes): 124997
Dropped Counter (Bytes): 10
Last drop time: 27-Jan-2014, 09:00:01
Multicast
Rate: 1000 kbps
Action: Drop, Trap
Passed Counter (Bytes):112876
Dropped Counter (Bytes):1272
Last drop time: 20-Jan-2014, 11:00:01
Unicast
Rate: 10%
Action: drop
Passed Counter (Bytes): 27653
Dropped Counter (Bytes):1
Last drop time: 27-Feb-2014, 09:00:01 te1/0/2
Broadacst
Rate: 5%
Action: Shutdown
Passed Counter (Bytes): 124997
Dropped Counter (Bytes): 0 Last drop time:
Multicast Unregistred
Rate: 5%
Action: Shutdown
Traffic Type:Broadcast
Passed Counter (Bytes): 124997
Dropped Counter (Bytes): 3
Last drop time: 26-Jan-2014, 10:00:01
```

44. RIP Commands

44.1. clear rip statistics

The `clear rip statistics` Privileged EXEC mode command clears statistics counters of all interfaces and all peers.

Syntax

- clear rip statistics

Parameters

- N/A

Command Mode

Privileged EXEC mode

Example

The following example shows how to clear all counters:

```
switchxxxxxx# clear rip statistics
```

44.2. default-information originate

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.

Syntax

- default-information originate
- no default-information originate

Parameters

N/A

Default Configuration

Default route is not generated by RIP.

Command Mode

Router RIP Configuration mode

User Guidelines

Use the command to enable generation of a default route.

Examples

Example 1 - The following example shows how to originate a default route:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# default-information originate switchxxxxxx(config-rip)#
exit
```

44.3. default-metric

The `default-metric` Router RIP configuration mode command sets the default metric value when RIP advertises routes derived by other protocols (for example, by static configuration). The no format of the command sets the default value.

Syntax

- default-metric [metric-value]
- no default-metric

Parameters

- metric-value - Default metric value (Range: 1-15)

Default Configuration

The default metric value is 1.

Command Mode

Router RIP Configuration mode

Example

The following example shows how to set the default metric to 2:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# default-metric 2
switchxxxxxx(config-rip)# exit
```

44.4. ip rip authentication key-chain

The `ip rip authentication key-chain` IP Interface Configuration mode command specifies the set of keys that can be used for and specifies the type of authentication. The no format of the command returns to default.

Syntax

- ip rip authentication key-chain name-of-chain
- no ip rip authentication key-chain

Parameters

- name-of-chain - Specifies the name of key set. The name-change parameter points to list of keys specified by the key chain CLI command.

Default Configuration

No defined key chain.

Command Mode

IP Configuration mode

User Guidelines

Use the `ip rip authentication key-chain` IP Interface Configuration mode command to define a key chain name. Only one key chain may be defined per an IP interface. Each `ip rip authentication key-chain` command overrides the previous definition.

In order to have a smooth rollover of keys in a key chain, a key should be configured with a lifetime that starts several minutes before the lifetime of the previous key expires.

Example

The following example shows how to define a chain name:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip authentication key-chain alpha
switchxxxxxx(config-route-map)# exit
```

44.5. ip rip authentication mode

The `ip rip authentication mode` IP Interface Configuration mode command enables authentication. The no formt of the command returns to default.

Syntax

- ip rip authentication mode {text | md5}
- no ip rip authentication mode

Parameters

- text - Specifies the clear text authentication.
- md5 - Specifies the MD5 authentication.

Default Configuration

No authentication.

Command Mode

IP Configuration mode

User Guidelines

If you enable the MD5 authentication, you must configure a key chain name with the `ip rip authentication key-chain` interface command. If a key chain is not defined for the IP interface or there is not a valid key then RIP packets are not sent on the IP interface and received IP interface packets are dropped.

If you enable the clear text authentication, you must configure a password with the `ip rip authentication-key` interface command. If a password is not defined for the IP interface then RIP packets are not sent on the IP interface and received IP interface packets are dropped.

Example

The following example shows how to set the md5 mode:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip authentication mode md5
switchxxxxxx(config-route-map)# exit
```

44.6. ip rip authentication-key

To assign a password to be used by neighboring routers that are using the RIP clear text authentication, use the `ip rip authentication-key` command in interface configuration mode. To remove the RIP password, use the no form of this command.

Syntax

- ip rip authentication-key password
- no ip rip authentication-key

Parameters

- password - Any continuous string of characters that can be entered from the keyboard up to 16 characters in length.

Default Configuration

No password is specified.

Command Mode

IP Configuration mode

User Guidelines

The password created by this command is used as a "key" that is inserted directly into the RIP header when the switch software originates routing protocol packets.

A separate password can be assigned to each subnetwork. All neighboring routers on the same subnetwork must have the same password to be able to exchange RIP information.

Only one password may be defined per IP interface. Each `ip rip authentication-key` command overrides the previous definition.

Example

The following example shows how to define a password:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip authentication mode text
switchxxxxxx(config-route-map)# ip rip authentication-key alph$$12
switchxxxxxx(config-route-map)# exit
```

44.7. ip rip default-information originate

The `ip rip default-information originate` IP Interface generates a metric for a default route in RIP. The no format of the command disables the feature.

Syntax

- ip rip default-information originate {disable | metric}
- no ip rip default-information originate

Parameters ranges

- disable - Do not send the default route.
- Metric - Default route metric value (Range: 1-15).

Default Configuration

The RIP behavior is specified by the default-information originate command.

Command Mode

IP Configuration mode

Use the command to override the RIP behavior specified by the default-information originate command on a given IP interface.

Example

The following example shows how to enable sending of default route with metric 3:

```
switchxxxxxx(config)# interface ip 1.1.1.1
```

```
switchxxxxxx(config-route-map)# ip rip default-information originate 3
switchxxxxxx(config-route-map)# exit
```

44.8. ip rip distribute-list in

The `ip rip distribute-list in` IP configuration mode command enables filtering of routes in incoming RIP update messages. The no format of the command disables the filtering.

Syntax

- ip rip distribute-list access access-list-name in
- no ip rip distribute-list in

Parameters

- access-list-name - Standard IP access list name, up to 32 characters. The list defines which routes in incoming RIP update messages are to be accepted and which are to be suppressed.

Default Configuration

No filtering

Command Mode

IP Configuration mode

Each network from a received RIP update message is evaluated by the access list and it is accepted only if it is permitted by the list. See the commands `ip access-list` (IP standard) and `ip prefix-list` for details.

Example

The following example shows how to define input filtering:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip distribute-list access 5 in
switchxxxxxx(config-route-map)# exit
```

44.9. ip rip distribute-list out

The `ip rip distribute-list out` IP configuration mode command enables filtering of routes in outgoing RIP update messages. The no format of the command disables the filtering.

Syntax

- ip rip distribute-list access access-list-name out
- no ip rip distribute-list out

Parameters

- access-list-name - Standard IP access list name, up to 32 characters. The list defines which routes in outgoing RIP update messages are to be sent and which are to be suppressed.

Default Configuration

No filtering

Command Mode

IP Configuration mode

Each network from the IP Forwarding table is evaluated by the list and it is included in the RIP update message only if it is permitted by the list. See the commands `ip access-list` (IP standard) and `ip prefix-list`.

Example

The following example shows how to define outgoing filtering:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip distribute-list access 5 out
switchxxxxxx(config-route-map)# exit
```

44.10. ip rip offset

The `ip rip offset` IP configuration mode command defines a metric added to incoming routes. The no format of the command returns to default.

Syntax

- ip rip offset offset
- no ip rip offset

Parameters

- offset - Specifies the offset to be applied to received routes (Range: 1-15).

Default Configuration

The default offset is 1.

Command Mode

IP Configuration mode

Example

The following example shows how to set offset to 2:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip offset 2
switchxxxxxx(config-route-map)# exit
```

44.11. ip rip passive-interface

The `ip rip passive-interface` IP Interface Configuration mode command disables sending RIP packets on an IP interface. The no format of the command re-enables the sending RIP packets.

Syntax

- ip rip passive-interface
- no ip rip passive-interface

Parameters

N/A.

Default Configuration

RIP messages are sent.

Command Mode

IP Configuration mode

User Guidelines

Use the `ip rip passive-interface` command to stop sending RIP messages on the giving IP interface. To stop RIP messages being sent on all interfaces, use the `passive-interface` command.

Note:
The `no ip rip passive-interface` command does not override the `passive-interface` command.

Example

The following example shows how to stop the sending of RIP messages:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip passive-interface
switchxxxxxx(config-route-map)# exit
```

44.12. ip rip shutdown

The `ip rip shutdown` IP Interface configuration mode command changes the RIP interface state from enabled to disabled. The no format of the command returns the state to a value of enabled.

Syntax

- ip rip shutdown
- no ip rip shutdown

Parameters

N/A

Default Configuration

Enabled

Command Mode

IP Configuration mode

User Guidelines

Use the `ip rip shutdown` CLI command to disable RIP on an IP interface without removing its configuration.The `ip rip shutdown` CLI command may be applied only to RIP interfaces created by the network CLI command. The `ip rip shutdown` CLI command does not remove the RIP interface configuration.

Example

The following example shows how to disable RIP on the 1.1.1.1 IP interface:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip shutdown
switchxxxxxx(config-route-map)# exit
```

44.13. network

The `network` Router RIP configuration mode command enables RIP on the given IP interfaces. The no format of the command disables RIP on the given IP interfaces and removes its interface configuration.

Syntax

- network ip-address [shutdown]
- no network ip-address

Parameters

- ip-address - An IP address of a switch IP interface.
- Shutdown - RIP is enabled on the interface in the shutdown state.

Default Configuration

N/A

Command Mode

Router RIP Configuration mode

User Guidelines

RIP can be defined only on manually-configured IP interfaces, meaning that RIP cannot be defined on an IP address defined by DHCP or on a default IP address.

Use the `network` CLI command with the shutdown keyword to create RIP on an interface if you are going to change the default values of RIP configuration and the use the no ip rip shutdown CLI command.

Use the `no network` CLI command to remove RIP on an IP interface and remove its interface configuration.

Examples

Example 1:

The following example shows how to enable RIP on IP interface 1.1.1.1 with the default interface configuration:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 1.1.1.1
switchxxxxxx(config-rip)# exit
```

Example 2:

The following example enables RIP on 1.1.1.1 in the shutdown state, configures metric and starts RIP:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 1.1.1.1 shutdown
switchxxxxxx(config-rip)# exit
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip offset 2
switchxxxxxx(config-route-map)# no ip rip shutdown
switchxxxxxx(config-route-map)# exit
```

44.14. passive-interface (RIP)

To disable sending routing updates on all RIP IP interfaces, use the `passive-interface` command in Router RIP Configuration mode. To re-enable the sending of RIP routing updates, use the no form of this command.

Syntax

- passive-interface
- no passive-interface

Parameters

N/A

Default Configuration

Routing updates are sent on all IP RIP interfaces.

Command Mode

Router RIP Configuration mode

User Guidelines

After using the passive-interface command, you can then configure individual interfaces where adjacencies are desired using the no ip rip passive-interface command.

Example

The following example sets all IP interfaces as passive and then excludes the IP interface 1.1.1.1:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# passive-interface
switchxxxxxx(config-rip)# network 1.1.1.1
switchxxxxxx(config-rip)# network 2.2.2.2
switchxxxxxx(config-rip)# network 3.3.3.3
switchxxxxxx(config-rip)# exit
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# no ip rip passive-interface
switchxxxxxx(config-route-map)# exit
```

44.15. redistribute (RIP)

To redistribute routes from one routing domain into a RIP routing domain, use the `redistribute` command in the Router RIP configuration mode. To disable redistribution, use the no form of this command.

Syntax

- redistribute protocol [process-id] [metric {metric-value | transparent}] [match {internal | external 1 | external 2}]
- no redistribute protocol [process-id] [match {internal | external 1 | external 2}]

Parameters

- protocol - Source protocol from which routes are being redistributed. It can be one of the following keywords: connected, static, or ospf.
- process-id - The process-id argument is used only together with the ospf keyword and specifies the appropriate OSPF process ID from which routes are to be redistributed.

This identifies the routing process. This value takes the form of a nonzero decimal number. If it is omitted then a value of 1 is assumed.

- metric transparent - Causes RIP to use the source protocol metric for redistributed routes as the RIP metric. Only routes with metric less than 16 are redistributed.
- metric metric-value - Specifies the metric assigned to the redistributed routes. The value supersedes the metric value specified using the default-metric command.
- match {internal | external 1 | external 2} The match keyword is used only together with the ospf keyword and specifies the criteria by which OSPF routes are redistributed into RIP. It can be one of the following:
  - internal - Routes that are internal to a specific autonomous system.
  - external 1 - Routes that are external to the autonomous system, but are imported into OSPF as Type 1 external route.
  - external 2 - Routes that are external to the autonomous system, but are imported into OSPF as Type 2 external route.

    By default the internal and external 1 routes are redistributed.

Note:
Multiple `redistribute` commands with various values of the match keyword may be defined.

Default Configuration

Route redistribution is disabled

Command Mode

Router RIP Configuration mode

User Guidelines

Routes distributed to the source protocol are never redistributed by it.

The connected keyword is used to redistribute to RIP routes that correspond to defined IP interfaces on which RIP is not enabled. By default, the RIP Routing Table includes only routes that correspond only to IP interfaces on which it is enabled.

The static keyword is used to redistribute to RIP static routes. By default, static routes are not redistributed to RIP.

If the metric value is set by the route map (by the `set metric` command) then the value will supersede the metric value specified by the metric-value argument.

If the metric keyword is not defined, then the metric is specified by the `default-metric` CLI command is assigned to the redistributed routes. If metric value set by the route map is equal or bigger than 16 the route is not redistributed.

Changing or disabling any keyword will not affect the state of other keywords.

Removing options that you have configured for the redistribute command requires careful use of the no form of the redistribute command to ensure that you obtain the result that you are expecting.

Examples

Example 1:

The following example enables redistribution of static routes by RIP with transparent metric:

```
switchxxxxxx(config)# router rip
```

```
switchxxxxxx(config-rip)# redistribute static metric transparent
 switchxxxxxx(config-rip)# exit
```

Example 2:

The following example enables redistribution of static routes by RIP with transparent metric and then changes the metric to default:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# redistribute static metric transparent
switchxxxxxx(config-rip)# no redistribute static metric transparent
switchxxxxxx(config-rip)# exit
```

Example 3:

The following example enables redistribution of static routes by RIP with default metric and then changes the metric to transparent:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# redistribute static
switchxxxxxx(config-rip)# redistribute static metric transparent
switchxxxxxx(config-rip)# exit
```

Example 4:

The following example enables redistribution of static routes by RIP with transparent metric. The second redistribute command does not affect:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# redistribute static metric transparent
switchxxxxxx(config-rip)# redistribute static
switchxxxxxx(config-rip)# exit
```

Example 5:

The following example disables redistribution of static routes by RIP:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# no redistribute static
switchxxxxxx(config-rip)# exit
```

Example 6:

The following example shows how internal and extenal 1 OSPF routes are redistributed into a RIP domain:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# redistribute ospf 1
switchxxxxxx(config-rip)# exit
```

Example 7:

The following example shows how internal and external 1 OSPF routes are redistributed into a RIP domain with metric 1 and external 2 OSPF routers with metric 4. The first redistribute command does not include the match keyword because it is a default value:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# redistribute ospf 1 metric 1
```

```
switchxxxxxx(config-rip)# redistribute ospf 1 match external 2 metric 4
switchxxxxxx(config-rip)# exit
```

44.16. router rip

The `router rip` Global Configuration mode command specifies the Router RIP mode and enables it if it was disabled. The no format of the command disables RIP globally and removes its configuration.

Syntax

- router rip
- no router rip

Parameters

N/A

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

RIP supports the following global states:

- disabled
- enabled
- shutdown

If a value of the RIP global state is disabled (default value), RIP is not operational and cannot be configured. When this state is set, the RIP configuration is removed. The state may be set by the no router rip CLI command from any RIP global state.

If a value of the RIP global state is shutdown, RIP is not operational, but can be configured. When the state is set the RIP configuration is not changed. The state may be set by the shutdown CLI command from the enabled RIP global state.

If the value of the RIP global state is enabled, RIP is operational, and can be configured. The state can be set by the router rip CLI command from the disabled RIP global state and by the no shutdown CLI command from the shutdown RIP global state.

Example

The following example shows how to enable RIP globally:

```
switchxxxxxx(config)# router rip
```

44.17. show ip rip database

The `show ip rip database` Privileged EXEC mode command displays information about the RIP Database.

Syntax

- show ip rip database [all | brief | ip-address]

Parameters

- all - Provides the full RIP database information about all RIP interfaces. The option is assumed if the parameter is omitted.
- Brief - Provides a summary view of the RIP database information.
- ip-address - Provides the full RIP database information about the given IP Address.

Command Mode

Privileged EXEC mode

Default Configuration

N/A

Examples

Example 1:

The following example shows the full RIP database information about all RIP interfaces is displayed:

```
switchxxxxxx# show ip rip database
RIP is enabled
RIP Administrative state is UP Default metric value is 1 Redistributing is
enabled from
  Connected:
    Metric is default-metric   Static:
    Metric is transparent   OSPF 109:     internal:
      metric value is 2     external 1:
      metric value is 4     external 2:       metric value is 6       with
subnets
IP Interface: 1.1.1.1
Administrative State is enabled
IP Interface Offset is 10
Default Originate Metric is 12
Authentication Type is text
Password is afGRwitew%3
IN Filtering Type is Access List
Access List Name is 10
OUT Filtering Type is Access List
Access List Name is List12
IP Interface: 2.2.2.2
Administrative State is enabled
IP Interface Offset is 2
No Default Originate Metric
Authentication Type is MD5
Key Chain Name is chain1
IN Filtering Type is Access List
Access List Name is 10
OUT Filtering Type is Access List
Access List Name is 12
IP Interface: 3.3.3.3
Administrative State is enabled
IP Interface Offset is 1
IP Interface is passive
Default Originate Metric 3, on passive too
No Authentication
No IN Filtering
```

```
No OUT Filtering
IP Interface: 4.4.4.4
Administrative State is shutdown
IP Interface Offset is 1
No Authentication No IN Filtering
No OUT Filtering
```

Example 2:

The following example shows the full RIP database information about a given IP address is displayed:

```
switchxxxxxx# show ip rip database 1.1.1.1
RIP is enabled
RIP Administrative state is UP
Default Originate Metric: on passive only
Default metric value is 1
Redistributing is enabled from
  Connected
   Metric is default-metric
  Static
   Metric is transparent   OSPF:
    from metric type:       metric value is 2     external 1       metric value is 4
external 2       metric value is 6       with subnets
IP Interface: 1.1.1.1
Administrative State is enabled
IP Interface Offset is 10
Default Originate Metric is 12
Authentication Type is text
Password is afGRwitew%3
IN Filtering Type is Access List
Access List Name is 10
OUT Filtering Type is Access List
Access List Name is List12
```

Example 3:

The following example shows the brief RIP database information about all RIP interfaces is displayed:

```
switchxxxxxx# show ip rip database brief
RIP is enabled
RIP Administrative state is UP
Default Originate Metric: route-map is condition
Default metric value is 1
Redistributing is enabled from
  Connected
   Metric is default-metric
  Static
   Metric is transparent   OSPF:
    from metric type:       metric value is 2     external 1       metric value is 4
external 2       metric value is 6       with subnets
IP Interface    Admin    Offset  Passive   Default Auth.  IN Filt. OUT Filt.
State            Interface Metric  Type    Type     Type
--------------- -------- ------- --------  ------- -----  -------  ---------
```

```
100.100.100.100 enabled    10      No          12    Text    Access   Access
2.2.2.2         enabled     2      No                MD5     Access   Access
3.3.3.3         enabled     1      Yes
4.4.4.4         shutdown    1      No
```

Example 4:

The following example shows the output when RIP is disabled:

```
switchxxxxxx# show ip rip database
RIP is disabled
```

44.18. show ip rip peers

The `show ip rip peers` Privileged EXEC mode command displays information about RIP Peers.

Syntax

- show ip rip peers

Parameters

N/A

Command Mode

Privileged EXEC mode

Default Configuration

N/A

Example

```
switchxxxxxx# show ip rip peers
RIP is enabled
Static redistributing is enabled with Default metric
Default redistributing metric is 1
Address       Last          Received       Received
              Update        Bad Packets    Bad Route
------------  ---------     ----------     ---------
1.1.12        00:10:17          -                1
2.2.2.3       00:10:01          -              -
```

44.19. show ip rip statistics

The `show ip rip statistics` Privileged EXEC mode command displays RIP statistics.

Syntax

- show ip rip statistics

Parameters

N/A

Command Mode

Privileged EXEC mode

Default Configuration

N/A

Example

```
switchxxxxxx# show ip rip statistics
RIP is enabled
Static redistributing is enabled with transparent metric
Default redistributing metric is 1
Interface     Received       Received           Sent
              Bad            Bad                Triggered
              Pakets         Routes             Packets
------------  -------------  -------------      -----------
1.1.1.1            -                  1              8
2.2.2.2            -                  -              7
```

44.20. shutdown

The `shutdown` Router RIP configuration mode command sets the RIP global state to shutdown. The no format of the command sets the RIP global state to enabled.

Syntax

- shutdown
- no shutdown

Parameters

N/A

Default Configuration

Enabled

Command Mode

Router RIP Configuration mode

User Guidelines

Use the `shutdown` CLI command to stop RIP globally without removing its configuration

Example

The following example shows how to shutdown RIP globally:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# shutdown
switchxxxxxx(config-rip)# exit
```

45. Remote Network Monitoring (RMON) Commands

45.1. rmon alarm

To configure alarm conditions, use the `rmon alarm` Global Configuration modecommand. To remove an alarm, use the no form of this command.

Syntax

- rmon alarm index mib-object-id interval rising-threshold falling-threshold rising-event falling-event [type {absolute | delta}] [startup {rising | rising-falling | falling}] [owner name]
- no rmon alarm index

Parameters

- index - Specifies the alarm index. (Range: 1–65535)
- mib-object-id - Specifies the object identifier of the variable to be sampled. (Valid OID)
- interval - Specifies the interval in seconds during which the data is sampled and compared with rising and falling thresholds. (Range: 1– 2147483647)
- rising-threshold - Specifies the rising threshold value. (Range: 0– 2147483647)
- falling-threshold - Specifies the falling threshold value. (Range: 0– 2147483647)
- rising-event - Specifies the index of the event triggered when a rising threshold is crossed. (Range: 0–65535)
- falling-event - Specifies the index of the event triggered when a falling threshold is crossed. (Range: 0–65535)
- type {absolute | delta} - (Optional) Specifies the method used for sampling the selected variable and calculating the value to be compared against the thresholds. The possible values are:
  - absolute - Specifies that the selected variable value is compared directly with the thresholds at the end of the sampling interval.
  - delta - Specifies that the selected variable value of the last sample is subtracted from the current value, and the difference is compared with the thresholds.
- startup {rising | rising-falling | falling} - (Optional) Specifies the alarm that may be sent when this entry becomes valid. The possible values are:
  - rising - Specifies that if the first sample (after this entry becomes valid) is greater than or equal to rising-threshold, a single rising alarm is generated.
  - rising-falling - Specifies that if the first sample (after this entry becomes valid) is greater than or equal to rising-threshold, a single rising alarm is generated. If the first sample (after this entry becomes valid) is less than or equal to falling-threshold, a single falling alarm is generated.
  - falling - Specifies that if the first sample (after this entry becomes valid) is less than or equal to falling-threshold, a single falling alarm is generated.
- owner name - (Optional) Specifies the name of the person who configured this alarm. (Valid string)

Default Configuration

The default method type is absolute.

The default startup direction is rising-falling.

If the owner name is not specified, it defaults to an empty string.

Command Mode

Global Configuration mode

Example

The following example configures an alarm with index 1000, MIB object ID D-Link, sampling interval 360000 seconds (100 hours), rising threshold value 1000000, falling threshold value 1000000, rising threshold event index 10, falling threshold event index 10, absolute method type and rising-falling alarm.

```
switchxxxxxx(config)# rmon alarm 1000 1.3.6.1.2.1.2.2.1.10.1 360000 1000000
1000000 10 20
```

45.2. show rmon alarm-table

To display a summary of the alarms table, use the `show rmon alarm-table` Privileged EXEC mode command.

Syntax

- show rmon alarm-table

Parameters

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

Example

The following example displays the alarms table.

```
switchxxxxxx# show rmon alarm-table
Index OID   Owner
----- ---------------------- -------
1.3.6.1.2.1.2.2.1.10.1 CLI
1.3.6.1.2.1.2.2.1.10.1 Manager
1.3.6.1.2.1.2.2.1.10.9 CLI
```

The following table describes the significant fields shown in the display:

Field	Description
Index	An index that uniquely identifies the entry.
OID	Monitored variable OID.
Owner	The entity that configured this entry.

45.3. show rmon alarm

To display alarm configuration, use the `show rmon alarm` Privileged EXEC mode command.

Syntax

- show rmon alarm number

Parameters

- alarm number - Specifies the alarm index. (Range: 1–65535)

Command Mode

Privileged EXEC mode

Example

The following example displays RMON 1 alarms.

```
switchxxxxxx# show rmon alarm 1
Alarm 1 -------
OID: 1.3.6.1.2.1.2.2.1.10.1
Last sample Value: 878128
Interval: 30
Sample Type: delta
Startup Alarm: rising
Rising Threshold: 8700000
Falling Threshold: 78
Rising Event: 1
Falling Event: 1
Owner: CLI
```

The following table describes the significant fields shown in the display:

Field	Description
Alarm	Alarm index.
OID	Monitored variable OID.
Last Sample Value	Value of the statistic during the last sampling period. For example, if the sample type is delta, this value is the difference between the samples at the beginning and end of the period. If the sample type is absolute, this value is the sampled value at the end of the period.
Interval	Interval in seconds over which the data is sampled and compared with the rising and falling thresholds.
Sample Type	Method of sampling the variable and calculating the value compared against the thresholds. If the value is absolute, the variable value is compared directly with the thresholds at the end of the sampling interval. If the value is delta, the variable value at the last sample is subtracted from the current value, and the difference is compared with the thresholds.
Startup Alarm	Alarm that is sent when this entry is first set. If the first sample is greater than or equal to the rising threshold, and startup alarm is equal to rising or rising-falling, then a single rising alarm is generated. If the first sample is less than or equal to the falling threshold, and startup alarm is equal falling or rising-falling, then a single falling alarm is generated.
Rising Threshold	Sampled statistic rising threshold. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated.
Falling Threshold	Sampled statistic falling threshold. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is

	greater than this threshold, a single event is generated.
Rising Event	Event index used when a rising threshold is crossed.
Falling Event	Event index used when a falling threshold is crossed.
Owner	Entity that configured this entry.

45.4. rmon event

To configure an event, use the `rmon event` Global Configuration modecommand.

To remove an event, use the no form of this command.

Syntax

- rmon event index {none | log | trap | log-trap} [community text] [description text] [owner name]
- no rmon event index

Parameters

- index - Specifies the event index. (Range: 1–65535)
  - none - Specifies that no notification is generated by the device for this event.
  - log - Specifies that a notification entry is generated in the log table by the device for this event.
  - trap - Specifies that an SNMP trap is sent to one or more management stations by the device for this event.
  - log-trap - Specifies that an entry is generated in the log table and an SNMP trap is sent to one or more management stations by the device for this event.
- community text - (Optional) Specifies the SNMP community (password) used when an SNMP trap is sent. (Octet string; length: 0–127 characters). Note this must be a community used in the definition of an SNMP host using the “snmp-server host” command.
- description text - (Optional) Specifies a comment describing this event. (Length: 0–127 characters)
- owner name - (Optional) Specifies the name of the person who configured this event. (Valid string)

Default Configuration

If the owner name is not specified, it defaults to an empty string.

Command Mode

Global Configuration mode

Example

The following example configures an event identified as index 10, for which the device generates a notification in the log table.

```
switchxxxxxx(config)# rmon event 10 log
```

45.5. show rmon events

To display the RMON event table, use the `show rmon events` Privileged EXEC mode command.

Syntax

- show rmon events

Parameters

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

Example

The following example displays the RMON event table.

```
switchxxxxxx# show rmon events
Index Description Type Community Owner Last time sent
----- ----------- ---- --------- ----- --------------
1 Errors Log router CLI Jan 18 2006 23:58:17
2 High Log Manager Jan 18 2006 23:59:48
 Broadcast Trap
```

The following table describes significant fields shown in the display:

Field	Description
Index	Unique index that identifies this event.
Description	Comment describing this event.
Type	Type of notification that the device generates about this event. Can have the following values: none, log, trap, log-trap. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations.
Community	If an SNMP trap is to be sent, it is sent with the SNMP community string specified by this octet string.
Owner	The entity that configured this event.
Last time sent	The time this entry last generated an event. If this entry has not generated any events, this value is zero.

45.6. show rmon log

To display the RMON log table, use the `show rmon log` Privileged EXEC mode command.

Syntax

- show rmon log [event]

Parameters

- event - (Optional) Specifies the event index. (Range: 0–65535)

Command Mode

Privileged EXEC mode

Example

The following example displays event 1 in the RMON log table.

switchxxxxxx# show rmon log 1

```
Maximum table size: 500 (800 after reset)
Event Description  Time
----- -------------    -------------------
1     MIB Var.:   Jan 18 2006 23:48:19
1.3.6.1.2.1.2.2.1.10.
53, Delta, Rising,
Actual Val: 800,
Thres.Set: 100,
Interval (sec):1
```

45.7. rmon table-size

To configure the maximum size of RMON tables, use the `rmon table-size` Global Configuration modecommand. To return to the default size, use the no form of this command.

Syntax

- rmon table-size {history entries | log entries}
- no rmon table-size {history | log}

Parameters

- history entries - Specifies the maximum number of history table entries. (Range: 20–32767)
- log entries - Specifies the maximum number of log table entries. (Range: 20–32767)

Default Configuration

The default history table size is 270 entries.

The default log table size is 200 entries.

Command Mode

Global Configuration mode

User Guidelines

The configured table size takes effect after the device is rebooted.

Example

The following example configures the maximum size of RMON history tables to 100 entries.

```
switchxxxxxx(config)# rmon table-size history 100
```

45.8. show rmon statistics

To display RMON Ethernet statistics, use the `show rmon statistics` Privileged EXEC mode command.

Syntax

- show rmon statistics {interface-id}

Parameters

- interface-id - Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

Privileged EXEC mode

Example

The following example displays RMON Ethernet statistics for port `te1/0/1`.

```
switchxxxxxx# show rmon statistics te1/0/1
Port te1/0/1
Dropped: 0
Octets: 0 Packets: 0
Broadcast: 0 Multicast: 0
CRC Align Errors: 0 Collisions: 0
Undersize Pkts: 0 Oversize Pkts: 0
Fragments: 0 Jabbers: 0
64 Octets: 0 65 to 127 Octets: 1
128 to 255 Octets: 1 256 to 511 Octets: 1
512 to 1023 Octets: 0 1024 to max Octets: 0
```

The following table describes the significant fields displayed.

Field	Description
Dropped	Total number of events in which packets were dropped by the probe due to lack of resources. Note that this number is not necessarily the number of packets dropped. It is the number of times this condition was detected.
Octets	Total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	Total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broadcast	Total number of good packets received and directed to the broadcast address. This does not include multicast packets.
Multicast	Total number of good packets received and directed to a multicast address. This number does not include packets directed to the broadcast address.
CRC Align Errors	Total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Collisions	Best estimate of the total number of collisions on this Ethernet segment.
Undersize Pkts	Total number of packets received, less than 64 octets long (excluding framing bits, but including FCS octets) and otherwise well formed.
Oversize Pkts	Total number of packets received, longer than 1518 octets (excluding framing bits, but including FCS octets) and otherwise well formed.
Fragments	Total number of packets received, less than 64 octets in length (excluding framing bits but including FCS octets) and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Jabbers	Total number of packets received, longer than 1518 octets (excluding framing bits, but including FCS octets), and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
64 Octets	Total number of packets (including bad packets) received that are 64 octets in length (excluding framing bits but including FCS octets).
65 to 127 Octets	Total number of packets (including bad packets) received that are between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128 to 255 Octets	Total number of packets (including bad packets) received that are between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256 to 511 Octets	Total number of packets (including bad packets) received that are between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512 to 1023 Octets	Total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024 to max	Total number of packets (including bad packets) received that were between 1024 octets and the maximum frame size in length inclusive (excluding framing bits but including FCS octets).

45.9. rmon collection stats

To enable RMON MIB collecting history statistics (in groups) on an interface, use the `rmon collection stats` Interface Configuration mode command. To remove a specified RMON history group of statistics, use the no form of this command.

Syntax

- rmon collection stats index [owner ownername] [buckets bucket-number] [interval seconds]
- no rmon collection stats index

Parameters

- index - The requested group of statistics index (Range: 1–65535).
- owner ownername - (Optional) Records the name of the owner of the RMON group of statistics. If unspecified, the name is an empty string (Range: Valid string).
- buckets bucket-number - (Optional) A value associated with the number of buckets specified for the RMON collection history group of statistics. If unspecified, defaults to 50 (Range: 1–50).
- interval seconds - (Optional) The number of seconds in each polling cycle.

If unspecified, defaults to 1800 (Range: 1–3600).

Command Mode

Interface Configuration mode.

45.10. show rmon collection stats

To display the requested RMON history group statistics, use the `show rmon collection stats` Privileged EXEC mode command.

Syntax

- show rmon collection stats [interface-id]

Parameters

- interface-id - (Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

Privileged EXEC mode

Example

The following example displays all RMON history group statistics.

```
switchxxxxxx# show rmon collection stats
Index Interface Interval Requested Samples Granted Samples Owner
----- --------- -------- ----------------- --------------- -----
1 te1/0/1 30 50 50 CLI
2 te1/0/1 1800 50 50 Manager
```

The following table describes the significant fields shown in the display.

Field	Description
Index	An index that uniquely identifies the entry.
Interface	The sampled Ethernet interface.
Interval	The interval in seconds between samples.
Requested Samples	The requested number of samples to be saved.
Field	Description
Granted Samples	The granted number of samples to be saved.
Owner	The entity that configured this entry.

45.11. show rmon history

To display RMON Ethernet history statistics, use the `show rmon history` Privileged EXEC mode command.

Syntax

- show rmon history index {throughput | errors | other} [period seconds]

Parameters

- index - Specifies the set of samples to display. (Range: 1–65535)
  - throughput - Displays throughput counters.
  - errors - Displays error counters.

- other - Displays drop and collision counters.

- period seconds - (Optional) Specifies the period of time in seconds to display. (Range: 1–2147483647)

Command Mode

Privileged EXEC mode

Example

The following examples display RMON Ethernet history statistics for index 1:

```
switchxxxxxx# show rmon history 1 throughput
Sample Set: 1 Owner: CLI
Interface: te1/0/1 Interval: 1800
Requested samples: 50 Granted samples: 50
Maximum table size: 500
Time Octets Packets Broadcast Multicast Util
------------------- ------- ------- --------- --------- ----
Jan 18 2005 21:57:00 303595962 357568 3289 7287 19%
Jan 18 2005 21:57:30 287696304 275686 2789 5878 20%

switchxxxxxx# show rmon history 1 errors
Sample Set: 1 Owner: Me
Interface:te1/0/1 Interval: 1800
Requested samples: 50 Granted samples: 50
Maximum table size: 500 (800 after reset)
Time CRC Under Oversize Fragments Jabbers
 Align size
------------------- ----- ----- -------- --------- ----
Jan 18 2005 21:57:00 1 1 0 49 0
Jan 18 2005 21:57:30 1 1 0 27 0

switchxxxxxx# show rmon history 1 other
Sample Set: 1 Owner: Me
Interface: te1/0/1 Interval: 1800
Requested samples: 50 Granted samples: 50
Maximum table size: 500

Time Dropped Collisions
------------------- ------- ----------
Jan 18 2005 21:57:00 3 0
Jan 18 2005 21:57:30 3 0
```

The following table describes significant fields shown in the display:

Field	Description
Time	Date and Time the entry is recorded.
Octets	Total number of octets of data (including those in bad packets and excluding framing bits but including FCS octets) received on the network.
Packets	Number of packets (including bad packets) received during this sampling interval.
Broadcast	Number of good packets received during this sampling interval that were directed to the broadcast address.

Multicast	Number of good packets received during this sampling interval that were directed to a multicast address. This number does not include packets addressed to the broadcast address.
Utilization	Best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.
CRC Align	Number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize	Number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
Oversize	Number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.
Fragments	Total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error), or a bad FCS with a non-integral number of octets (Alignment Error). It is normal for etherHistoryFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.
Jabbers	Number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Dropped	Total number of events in which packets were dropped by the probe due to lack of resources during this sampling interval. This number is not necessarily the number of packets dropped, it is the number of times this condition has been detected.
Collisions	Best estimate of the total number of collisions on this Ethernet segment during this sampling interval.

46. RSA and Certificate Commands

46.1. Keys and Certificates

The device automatically generates default RSA/DSA keys and certificates at following times:

- When the device is booted with an empty configuration.
- When user-defined keys/certificates are deleted.

Some commands in this section are used to generate user-defined RSA/DSA keys and certificates that replace the default keys and are used by SSL and SSH server commands. Other commands can be used to import these keys from an external source.

These keys and certificates are stored in the configuration files.

The following table describes when these keys/certificates are displayed..

File Type Being Displayed	What is Displayed in a Show Command Without Detailed	What is Displayed in a Show Command With Detailed
Startup Config	Only user-defined keys/certificates.	Option is not supported.
Running Config	Keys are not displayed.	All keys (default and user-defined)
Text-based CLI (local backup config. file, or remote backup config. file)	Keys are displayed as they were copied. There is no distinction here between default and user-defined keys.	Option is not supported.

The following table describes how keys/certificates can be copied from one type of configuration file to another (using the copy command)..

Destination File Type	Copy from Running Config.	Copy from Startup Config.	Copy from Remote/Local Backup Config. File
Startup Config.	All keys/certificate s are copied (but only user-defined ones can be displayed	Option is not supporte d.	All keys/certificates present in this file are copied (*, **).
Running Config	N/A	Only user defined.	All keys/certificates present in this file are copied (*).
Text-based CLI (local backup config. file, or	All keys (default and user)	Only user defined.	All keys/certificates present in this file are copied (**)

remote backup config. file)			

* If the Running Configuration file on the device contains default keys (not user-defined ones), the same default keys remain after reboot.

** In a text-based configuration file, there is no distinction between automatically-defined, default keys and user-defined keys.

46.2. crypto key generate dsa

The crypto key generate dsa Global Configuration mode command generates a DSA key pair for SSH Public-Key authentication.

Syntax

- crypto key generate dsa

Parameters

N/A

Default Configuration

The application creates a default key automatically.

Command Mode

Global Configuration mode

User Guidelines

DSA keys are generated in pairs - one public DSA key and one private DSA key.

If the device already has DSA keys default or user defined, a warning is displayed with a prompt to replace the existing keys with new keys.

Erasing the startup configuration or returning to factory defaults automatically deletes the default keys and they are recreated during device initialization.

This command is not saved in the Running configuration file. However, the keys generated by this command are saved to the Running Configuration file.

See “Keys and Certificates” for information on how to display and copy this key pair.

Example

The following example generates a DSA key pair.

```
switchxxxxxx(config)# crypto key generate dsa
The SSH service is generating a private DSA key.
This may take a few minutes, depending on the key size.
..........
```

46.3. crypto key generate rsa

The crypto key generate rsa Global Configuration mode command generates RSA key pairs for SSH Public-Key Authentication.

Syntax

- crypto key generate rsa

Parameters

N/A

Default Configuration

The application creates a default key automatically.

Command Mode

Global Configuration mode

User Guidelines

RSA keys are generated in pairs - one public RSA key and one private RSA key.

If the device already has RSA keys default or user defined, a warning is displayed with a prompt to replace the existing keys with new keys.

Erasing the startup configuration or returning to factory defaults automatically deletes the default keys and they are recreated during device initialization.

This command is not saved in the Running configuration file. However, the keys generated by this command are saved to the Running Configuration file.

See Keys and Certificates for information on how to display and copy this key pair.

Example

The following example generates RSA key pairs where a RSA key already exists.

```
switchxxxxxx(config)# crypto key generate rsa Replace Existing RSA Key [y/n]? N
switchxxxxxx(config)#
```

46.4. crypto key import

The crypto key import Global Configuration mode command imports the DSA/RSA key pair.

Use the no form of the command to remove the user key and generate a new default in its place.

Syntax

- crypto key import {dsa | rsa}
- no crypto key {dsa | rsa}

Parameters

N/A

Default Configuration

DSA and RSA key pairs do not exist.

Command Mode

Global Configuration mode

User Guidelines

DSA/RSA keys are imported in pairs - one public DSA/RSA key and one private DSA/RSA key.

If the device already has DSA/RSA keys, a warning is displayed with a prompt to replace the existing keys with new keys.

This command is saved in the Running Configuration file.

Example

```
switchxxxxxx(config)# crypto key import rsa
---- BEGIN SSH2 PRIVATE KEY ---switchxxxxxx(config)# encrypted crypto key import
rsa
---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----
Comment: RSA Private Key
84et9C2XUfcRlpemuGINAygnLwfkKJcDM6m2OReALHScqqLhi0wMSSYNlT1IWFZP1kEVHH
Fpt1aECZi7HfGLcp1pMZwjn1+HaXBtQjPDiEtbpScXqrg6ml1/OEnwpFK2TrmUy0Iifwk8
E/mMfX3i/2rRZLkEBea5jrA6Q62gl5naRw1ZkOges+GNeibtvZYSk1jzr56LUr6fT7Xu5i
KMcU2b2NsuSD5yW8R/x0CW2elqDDz/biA2gSgd6FfnW2HV48bTC55eCKrsId2MmjbExUdz
+RQRhzjcGMBYp6HzkD66z8HmShOU+hKd7M1K9U4Sr+Pr1vyWUJlEkOgz9O6aZoIGp4tgm4
VDy/K/G/sI5nVL0+bR8LFUXUO/U5hohBcyRUFO2fHYKZrhTiPT5Rw+PHt6/+EXKG9E+TRs
lUADMltCRvs+lsB33IBdvoRDdl98YaA2htZay1TkbMqCUBdfl0+74UOqa/b+bp67wCYKe9
yen418MaYKtcHJBQmF7sUQZQGP34VPmOMyZzon68S/ZoT77cy0ihRZx9wcI1yYhJnDiYxP
dgXHYhW6kCTcTj6LrUSQuxCJ9su89ZIWNn5OwdgonLSpvfnabv2GHmmelaveL7JJ/7UcfO
61q5D4PJ67Vk2xL7PqyHXN931rseTzPuJplkSLCFZ5uqTMbWWyQEKmHDlOx35vlGou5tky
9LgIwG4d+9edctZZaggeq5cgjnsZWJgUoB4Bn4hIreyOdHDiFUPPRxkoyhGOGnJuvxC9T9
K6BF1wBTdDQS+Gu47/0/gRoD/50q4sGkzqHsRJJ53WOT0Q1bHMTMLPpwn2nXzvfGxWL/bu
QhZZSqRonG6MX1cP7KT7i4TPq2w2k3TGtNBnVYHx6OoNcaTHmg1N2s5OgRsyXD9tF++6nY
RfMN8CsV+9jQKQP7ZaGc8Ju+d72jvSwppSr032HY+IpzZ4ujkK+/X5oawZL5NnkaEQTQKX
RSL55S4O5NPOjS/pC9hg7GaVjoY2mQ7HDpSUBeTIDTlvOwC2kskA9C6aF/Axj2dXLweQd5
lxk7m0/mMNaiJsNk6y33LcuKjIxpNNjK9n9KzRPkGNMFObprfenWKteDftjQ==
---- END SSH2 PRIVATE KEY ----
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAABIwAAAIEAvRHsKry6NKMKymb+yWEp9042vupLvYVq3ngt1sB9JH
OcdK/2nw7lCQguy1mLsX8/bKMXYSk/3aBEvaoJQ82+r/nRf0y3HTy4Wp9zV0SiVC8jLD+7
7t0aHejzfUhr0FRhWWcLnvYwr+nmrYDpS6FADMC2hVA85KZRye9ifxT7otE=
---- END SSH2 PUBLIC KEY ----
```

46.5. show crypto key

The show crypto key Privileged EXEC mode command displays the device’s SSH public keys for both default and user-defined keys.

Syntax

- show crypto key [mypubkey] [rsa | dsa]

Parameters

- mypubkey - Displays only the public key.
- rsa - Displays the RSA key.
- dsa - Displays the DSA key.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

See Keys and Certificates for information on how to display and copy this key pair.

Example

The following example displays the SSH public DSA keys on the device.

```
switchxxxxxx# show crypto key mypubkey dsa
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAABIwAAAIEAzN31fu56KSEOZdrGVPIJHpAs8G8NDIkB
dqZ2q0QPiKCnLPw0Xsk9tTVKaHZQ5jJbXn81QZpolaPLJIIH3B1cc96D7IFf
VkbPbMRbz24dpuWmPVVLUlQy5nCKdDCui5KKVD6zj3gpuhLhMJor7AjAAu5e
BrIi2IuwMVJuak5M098=
---- END SSH2 PUBLIC KEY ----
Public Key Fingerprint: 6f:93:ca:01:89:6a:de:6e:ee:c5:18:82:b2:10:bc:1e
```

46.6. crypto certificate generate

The crypto certificate generate Global Configuration mode command generates a self-signed certificate for HTTPS.

Syntax

- crypto certificate number generate [key-generate [length]] [cn common- name] [ou organization-unit] [or organization] [loc location] [st state] [cu country] [duration days]

Parameters

- number - Specifies the certificate number. (Range: 1–2)
- key-generate length - Regenerates SSL RSA key and specifies the SSL's RSA key length. (Range: 2048–3072)

The following elements can be associated with the key. When the key is displayed, they are also displayed.

- cn common- name - Specifies the fully qualified device URL or IP address. (Length: 1–64 characters). If unspecified, defaults to the lowest IP address of the device (when the certificate is generated).
- ou organization-unit - Specifies the organization-unit or department name. (Length: 1–64 characters)
- or organization - Specifies the organization name. (Length: 1–64 characters)
- loc location - Specifies the location or city name. (Length: 1–64 characters)
- st state - Specifies the state or province name. (Length: 1–64 characters)
- cu country - Specifies the country name. (Length: 2 characters)
- duration days - Specifies the number of days a certification is valid. (Range: 30–3650)

Default Configuration

If the key-generate parameter is not used the certificate is generated using the existing key.

The default SSL's RSA key length is 2048.

If cn common- name is not specified, it defaults to the device's lowest static IPv6 address (when the certificate is generated), or to the device's lowest static IPv4 address if there is no static IPv6 address, or to 0.0.0.0 if there is no static IP address.

If duration days is not specified, it defaults to 365 days.

Command Mode

Global Configuration mode

User Guidelines

If the specific certificate key does not exist, you must use the parameter key-generate.

If both certificates 1 and 2 have been generated, use the ip https certificate command to activate one of them.

See Keys and Certificates for information on how to display and copy this key pair.

Erasing the startup configuration or returning to factory defaults automatically deletes the default keys and they are recreated during device initialization.

Example

The following example generates a self-signed certificate for HTTPS whose length is 2048 bytes.

```
switchxxxxxx(config)# crypto certificate 1 generate key-generate 2048
```

46.7. crypto certificate request

The crypto certificate request Privileged EXEC mode command generates and displays a certificate request for HTTPS.

Syntax

- crypto certificate number request [cn common- name] [ou organization-unit] [or organization] [loc location] [st state] [cu country]

Parameters

- number - Specifies the certificate number. (Range: 1–2)
- The following elements can be associated with the key. When the key is displayed, they are also displayed.
- cn common- name - Specifies the fully qualified device URL or IP address. (Length: 1–64 characters). If unspecified, defaults to the lowest IP address of the device (when the certificate is generated).
- ou organization-unit - Specifies the organization-unit or department name. (Length: 1–64 characters)
- or organization - Specifies the organization name. (Length: 1–64 characters)
- loc location - Specifies the location or city name. (Length: 1–64 characters)
- st state - Specifies the state or province name. (Length: 1–64 characters)
- cu country - Specifies the country name. (Length: 2 characters)

Default Configuration

If cn common-name is not specified, it defaults to the device’s lowest static IPv6 address (when the certificate is generated), or to the device’s lowest static IPv4 address if there is no static IPv6 address, or to 0.0.0.0 if there is no static IP address.

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to export a certificate request to a Certification Authority. The certificate request is generated in Base64-encoded X.509 format.

Before generating a certificate request, first generate a self-signed certificate using the crypto cerificate generate command to generate the keys. The certificate fields must be re-entered.

After receiving the certificate from the Certification Authority, use the crypto cerificate import command to import the certificate into the device. This certificate replaces the self-signed certificate.

Example

The following example displays the certificate request for HTTPS.

```
switchxxxxxx# crypto certificate 1 request
-----BEGIN CERTIFICATE REQUEST-----
MIwTCCASoCAQAwYjELMAkGA1UEBhMCUFAxCzAJBgNVBAgTAkNDMQswCQYDVQQH
EwRDEMMAoGA1UEChMDZGxkMQwwCgYDVQQLEwNkbGQxCzAJBgNVBAMTAmxkMRAw
DgKoZIhvcNAQkBFgFsMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8ecwQ
HdML0831i0fh/F0MV/Kib6Sz5p+3nUUenbfHp/igVPmFM+1nbqTDekb2ymCu6K
aKvEbVLF9F2LmM7VPjDBb9bb4jnxkvwW/wzDLvW2rsy5NPmH1QVl+8Ubx3GyCm
/oW93BSOFwxwEsP58kf+sPYPy+/8wwmoNtDwIDAQABoB8wHQYJKoZIhvcNAQkH
MRDjEyMwgICCAgICAICAgIMA0GCSqGSIb3DQEBBAUAA4GBAGb8UgIx7rB05m+2
m5ZZPhIwl8ARSPXwhVdJexFjbnmvcacqjPG8pIiRV6LkxryGF2bVU3jKEipcZa
g+uNpyTkDt3ZVU72pjz/fa8TF0n3
-----END CERTIFICATE REQUEST-----
```

46.8. crypto certificate import

The `crypto certificate import` Global Configuration mode command imports a certificate signed by a Certification Authority for HTTPS. In addition, the relevant key-pair can also be imported.

Use the no form of the command to delete the user-defined keys and certificate.

Syntax

- crypto certificate number import
- no crypto certificate number

Parameters

- number - Specifies the certificate number. (Range: 1–2).

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

Certificate needs to be imported from PEM encoding/file extension

To end the session (return to the command line to enter the next command), enter a blank line.

The imported certificate must be based on a certificate request created by the crypto cerificate request command.

If only the certificate is imported, and the public key found in the certificate does not match the device's SSL RSA key, the command fails. If both the public key and the certificate are imported, and the public key found in the certificate does not match the imported RSA key, the command fails.

This command is saved in the Running configuration file.

See Keys and Certificates for information on how to display and copy this key pair.

Examples

Example 1 - The following example imports a certificate signed by the Certification Authority for HTTPS.

```
switchxxxxxx(config)# crypto certificate 1 import
Please paste the input now, add a period (.) on a separate line after the
input,and press Enter.
-----BEGIN CERTIFICATE-----
MIIBkzCB/QIBADBUMQswCQYDVQQGEwIgIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMB
IDEVMBMGA1UEAxMMMTAuNS4yMzQuMjA5MQowCAYDVQQKEwEgMQowCAYDVQQLEwEg
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDK+beogIcke73sBSL7tC2DMZrY
OOg9XM1AxfOiqLlQJHd4xP+BHGZWwfkjKjUDBpZn52LxdDu1KrpB/h0+TZP0Fv38
7mIDqtnoF1NLsWxkVKRM5LPka0L/ha1pYxp7EWAt5iDBzSw5sO4lv0bSN7oaGjFA
6t4SW2rrnDy8JbwjWQIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAuqYQiNJst6hI
XFDxe7I8Od3Uyt3Dmf7KE/AmUV0Pif2yUluy/RuxRwKhDp/lGrK12tzLQz+s5Ox7
Klft/IcjzbBYXLvih45ASWG3TRv2WVKyWs89rPPXu5hKxggEeTvWqpuS+gXrIqjW
WVZd0n1fXhMacoflgnnEmweIzmrqXBs= .
-----END CERTIFICATE-----
Certificate imported successfully.
Issued by : C= , ST= , L= , CN=0.0.0.0, O= , OU=
 Valid From: Jan 24 18:41:24 2011 GMT
Valid to: Jan 24 18:41:24 2012 GMT
Subject: C=US , ST= , L= , CN=router.gm.com, O= General Motors, OU=
 SHA1 Finger print: DC789788 DC88A988 127897BC BB789788
```

Example 2:The following example imports a certificate signed by the Certification Authority for HTTPS, and the RSA key-pair.

```
switchxxxxxx(config)# crypto certificate 1 import
Please paste the input now, add a period (.) on a separate line after the
input,and press Enter.
-----BEGIN RSA PRIVATE KEY-----
ACnrqImEGlXkwxBuZUlAO9nHq9IGJsnkf7/MauGPVqxt5vfDf77uQ5CPf49JWQhu07cVXh
2OwrBhJgB69vLUlJujM9p1IXFpMk8qR3NS7JzlInYAWjHKKbEZBMsKSA6+t/UzVxevKK6H
TGB7vMxi+hv1bL9zygvmQ6+/6QfqA51c4nP/8a6NjO/ZOAgvNAMKNr2Wa+tGUOoAgL0b/C
11EoqzpCq5mT7+VOFhPSO4dUU+NwLv1YCb1Fb7MFoAa0N+y+2NwoGp0pxOvDA9ENYl7qsZ
MWmCfXu52/IxC7fD8FWxEBtks4V81Xqa7K6ET657xS7m8yTJFLZJyVawGXKnIUs6uTzhhW
dKWWc0e/vwMgPtLlWyxWynnaP0fAJ+PawOAdsK75bo79NBim3HcNVXhWNzqfg2s3AYCRBx
WuGoazpxHZ0s4+7swmNZtS0xI4ek43d7RaoedGKljhPqLHuzXHUon7Zx15CUtP3sbHl+XI
B3u4EEcEngYMewy5obn1vnFSot+d5JHuRwzEaRAIKfbHa34alVJaN+2AMCb0hpI3IkreYo
A8Lk6UMOuIQaMnhYf+RyPXhPOQs01PpIPHKBGTi6pj39XMviyRXvSpn5+eIYPhve5jYaEn
UeOnVZRhNCVnruJAYXSLhjApf5iIQr1JiJb/mVt8+zpqcCU9HCWQqsMrNFOFrSpcbHu5V4
ZX4jmd9tTJ2mhekoQf1dwUZbfYkRYsK70ps8u7BtgpRfSRUr7g0LfzhzMuswoDSnB65pkC
ql7yZnBeRS0zrUDgHLLRfzwjwmxjmwObxYfRGMLp4=
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBAMVuFgfJYLbUzmbm6UoLD3ewHYd1ZMXY4A3KLF2SXUd1TIXq84aME8DIitSfB2
Cqy4QB5InhgAobBKC96VRsUe2rzoNG4QDkj2L9ukQOvoFBYNmbzHc7a+7043wfVmH+QOXf
TbnRDhIMVrZJGbzl1c9IzGky1l21Xmicy0/nwsXDAgEj
-----END RSA PUBLIC KEY-----
-----BEGIN CERTIFICATE-----
MIIBkzCB/QIBADBUMQswCQYDVQQGEwIgIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMB
IDEVMBMGA1UEAxMMMTAuNS4yMzQuMjA5MQowCAYDVQQKEwEgMQowCAYDVQQLEwEg
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDK+beogIcke73sBSL7tC2DMZrY
OOg9XM1AxfOiqLlQJHd4xP+BHGZWwfkjKjUDBpZn52LxdDu1KrpB/h0+TZP0Fv38
7mIDqtnoF1NLsWxkVKRM5LPka0L/ha1pYxp7EWAt5iDBzSw5sO4lv0bSN7oaGjFA
```

```
6t4SW2rrnDy8JbwjWQIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAuqYQiNJst6hI
XFDxe7I8Od3Uyt3Dmf7KE/AmUV0Pif2yUluy/RuxRwKhDp/lGrK12tzLQz+s5Ox7
Klft/IcjzbBYXLvih45ASWG3TRv2WVKyWs89rPPXu5hKxggEeTvWqpuS+gXrIqjW
WVZd0n1fXhMacoflgnnEmweIzmrqXBs=
-----END CERTIFICATE----.
Certificate imported successfully.
Issued by : C= , ST= , L= , CN=0.0.0.0, O= , OU=
 Valid From: Jan 24 18:41:24 2011 GMT
Valid to: Jan 24 18:41:24 2012 GMT
Subject: C=US , ST= , L= , CN=router.gm.com, O= General Motors, OU= SHA1 Finger
print: DC789788 DC88A988 127897BC BB789788
```

46.9. show crypto certificate

The show crypto certificate Privileged EXEC mode command displays the device SSL certificates and key-pair for both default and user defined keys.

Syntax

- show crypto certificate [mycertificate] [number]

Parameters

- number - Specifies the certificate number. (Range: 1,2)

Default Configuration

displays both keys.

Command Mode

Privileged EXEC mode

Examples

The following example displays SSL certificate # 1 present on the device.

```
switchxxxxxx# show crypto certificate 1 Certificate 1:
Certificate Source: Default -----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAp4HS
nnH/xQSGA2ffkRBwU2XIxb7n8VPsTm1xyJ1t11a1GaqchfMqqe0kmfhcoHSWr
yf1FpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYeBABDAEEw
CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFAf4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASkwgdKggc+ggcyGgclsZGFwOi8v
L0VByb3h5JTIwU29mdHdhcmUlMjBSb290JTIwQ2VydGlmaWVyLENOPXNlcnZl
-----END CERTIFICATE-----
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
```

47. TACACS+ Commands

47.1. tacacs-server host

To specify up to 8 TACACS+ hosts, use the `tacacs-server host` Global Configuration mode command. To delete the specified TACACS+ host, use the no form of this command.

Syntax

- tacacs-server host {ip-address | hostname} [single-connection] [port port-number][timeout timeout] [key key-string] [priority priority]
- no tacacs-server host {ip-address | hostname}

Parameters

- host ip-address - Specifies the TACACS+ server host IP address. The IP address can be an IPv4, IPv6 or IPv6 address.
- host hostname - Specifies the TACACS+ server host name. (Length: 1-158 characters. Maximum label length of each part of the host name: 63 characters)
- single-connection - (Optional) Specifies that a single open connection is maintained between the device and the daemon, instead of the device opening and closing a TCP connection to the daemon each time it communicates.
- port port-number - (Optional) Specifies the TACACS server TCP port number. If the port number is 0, the host is not used for authentication. (Range: 0-65535)
- timeout timeout - (Optional) Specifies the timeout value in seconds. (Range: 1-30)
- key key-string - (Optional) Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. To specify an empty string, enter "". (Length: 0-128 characters). If this parameter is omitted, the globally-defined key (set in the tacacs-server key command `tacacs-server host source-interface` command) will be used.
- priority priority - (Optional) Specifies the order in which the TACACS+ servers are used, where 0 is the highest priority. (Range: 0-65535)

Default Configuration

No TACACS+ host is specified.

The default port-number is 1812.

If timeout is not specified, the global value (set in the tacacs-server timeout command) is used.

If key-string is not specified, the global value (set in the tacacs-server key command) is used.

Command Mode

Global Configuration mode

User Guidelines

Multiple tacacs-server host commands can be used to specify multiple hosts (up to 8).

Example

The following example specifies a TACACS+ host.

```
switchxxxxxx(config)# tacacs-server host 172.16.1.1
```

47.2. tacacs-server host source-interface

To specify the source interface which IPv4 address will be used as the Source IPv4 address for communication with IPv4 TACACS+ servers, use the `tacacs-server host source-interface` Global Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- tacacs-server host source-interface interface-id
- no tacacs-server host source-interface interface-id - Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the interface IP address belonging to next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface, the minimal IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 TACACS+ server.

OOB cannot be defined as a source interface.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# tacacs-server host source-interface vlan 100
```

47.3. tacacs-server host source-interface-ipv6

To specify the source interface whose IPv6 address will be used as the Source IPv6 address for communication with IPv6 TACACS+ servers, use the `tacacs-server host source-interface-ipv6` Global Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- tacacs-server host source-interface-ipv6 interface-id
- no tacacs-server host source-interface-ipv6

Parameters

- interface-id - Specifies the source interface.

Default Configuration

The IPv6 source address is the IPv6 address defined on the outgoing interface and selected in accordance with RFC6724.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the source IPv6 address is an IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

If the source interface is not the outgoing interface, the source IPv6 address is the minimal IPv6 address defined on the source interface and matched to the scope of the destination IPv6 address is applied.

If there is no available source IPv6 address, a SYSLOG message is issued when attempting to communicate with an IPv6 TACACS+ server.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# tacacs-server host source-interface-ipv6 vlan 100
```

47.4. tacacs-server key

To set the authentication encryption key used for all TACACS+ communications between the device and the TACACS+ daemon, use the `tacacs-server key` Global Configuration mode command. To disable the key, use the no form of this command.

Syntax

- tacacs-server key key-string
- no tacacs-server key

Parameters

- key-string - Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server.

This key must match the encryption used on the TACACS+ daemon. (Length: 0–128 characters)

Default Configuration

The default key is an empty string.

Command Mode

Global Configuration mode

Example

The following example sets Enterprise as the authentication key for all TACACS+ servers.

```
switchxxxxxx(config)# tacacs-server key enterprise
```

47.5. tacacs-server timeout

To set the interval during which the device waits for a TACACS+ server to reply, use the `tacacs-server timeout` Global Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- tacacs-server timeout timeout
- no tacacs-server timeout

Parameters

- timeout - Specifies the timeout value in seconds. (Range: 1-30).

Default Configuration

The default timeout value is 5 seconds.

Command Mode

Global Configuration mode

Example

The following example sets the timeout value to 30 for all TACACS+ servers.

```
switchxxxxxx(config)# tacacs-server timeout 30
```

47.6. show tacacs

To display configuration and statistical information for a TACACS+ server, use the `show tacacs` Privileged EXEC mode command.

Syntax

- show tacacs [ip-address]

Parameters

- ip-address - Specifies the TACACS+ server name, IPv4 or IPv6 address.

Default Configuration

If ip-address is not specified, information for all TACACS+ servers is displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays configuration and statistical information for all TACACS+ servers

```
switchxxxxxx# show tacacs
IP address Status Port Single Time Priority
 Connection Out
--------- --------- ---- --------- ------ --------
172.16.1.1 Connected 49 No Global 1
Global values
-------------
Time Out: 3
Source IPv4 interface: vlan 120
Source IPv6 interface: vlan 10
```

47.7. show tacacs key

To display the configured key of the TACACS+ server, use the `show tacacs key` Privileged EXEC mode command.

Syntax

- show tacacs key [ip-address]

Parameters

- ip-address - Specifies the TACACS+ server name or IP address.

Default Configuration

If ip-address is not specified, information for all TACACS+ servers is displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays configuration and statistical information for all TACACS+ servers

```
switchxxxxxx# show tacacs key
IP address Key
---------- ---
172.16.1.1 Sharon123
172.16.1.2 Bruce123

Global key
-------------
Alice456
```

48. Telnet, Secure Shell (SSH) and Secure Login (Slogin) Commands

48.1. ip telnet server

Use the `ip telnet server` Global Configuration mode command to enable the device as a Telnet server that accepts up to 5 connection requests from remote Telnet clients. Remote Telnet clients can configure the device through the Telnet connections.

Use the no form of this command to disable the Telnet server functionality on the device.

Syntax

- ip telnet server
- no ip telnet server

Default Configuration

Enabled

Command Mode

Global Configuration mode

User Guidelines

The device can be enabled to accept connection requests from both remote SSH and Telnet clients. It is recommended that the remote client connects to the device using SSH (as opposed to Telnet), since SSH is a secure protocol and Telnet is not. To enable the device to be an SSH server, use the `ip ssh server` command.

Example

The following example enables the device to be configured from a Telnet server.

```
switchxxxxxx(config)# ip telnet server
```

48.2. ip ssh server

The `ip ssh server` Global Configuration mode command enables the device to be an SSH server and so to accept up to 4 connection requests from remote SSH clients. Remote SSH clients can manage the device through the SSH connection.

Use the no form of this command to disable the SSH server functionality from the device.

Syntax

- ip ssh server
- no ip ssh server

Default Configuration

The SSH server functionality is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

The device, as an SSH server, generates the encryption keys automatically.

To generate new SSH server keys, use the crypto key generate dsa and crypto key generate rsa commands.

Example

The following example enables configuring the device to be an SSH server.

```
switchxxxxxx(config)# ip ssh server
```

48.3. ip ssh port

The `ip ssh port` Global Configuration mode command specifies the TCP port used by the SSH server. Use the no form of this command to restore the default configuration.

Syntax

- ip ssh port port-number
- no ip ssh port

Parameters

- port-number - Specifies the TCP port number to be used by the SSH server. (Range: 1–65535).

Default Configuration

The default TCP port number is 22.

Command Mode

Global Configuration mode

Example

The following example specifies that TCP port number 8080 is used by the SSH server.

```
switchxxxxxx(config)# ip ssh port 8080
```

48.4. ip ssh password-auth

Use the `ip ssh password-auth` Global Configuration mode command to enable password authentication of incoming SSH sessions.

Use the no form of this command to disable this function.

Syntax

- ip ssh password-auth
- no ip ssh password-auth

Default Configuration

Password authentication of incoming SSH sessions is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables password key authentication by a local SSH server of remote SSH clients.

The local SSH server advertises all enabled SSH authentication methods and remote SSH clients are responsible for choosing one of them.

After a remote SSH client is successfully authenticated by public key, the client must still be AAA-authenticated to gain management access to the device.

If no SSH authentication method is enabled, remote SSH clients must still be AAA-authenticated before being granted management access to the device.

Example

The following example enables password authentication of the SSH client.

```
switchxxxxxx(config)# ip ssh password-auth
```

48.5. ip ssh pubkey-auth

Use the `ip ssh pubkey-auth` Global Configuration mode command to enable public key authentication of incoming SSH sessions.

Use the no form of this command to disable this function.

Syntax

- ip ssh pubkey-auth [auto-login]
- no ip ssh pubkey-auth

Parameters

- auto-login - Specifies that the device management AAA authentication (CLI login) is not needed. By default, the login is required after the SSH authentication.

Default Configuration

Public key authentication of incoming SSH sessions is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables public key authentication by a local SSH server of remote SSH clients.

The local SSH server advertises all enabled SSH authentication methods and remote SSH clients are responsible for choosing one of them.

After a remote SSH client is successfully authenticated by public key, the client must still be AAA-authenticated to gain management access to the device, except if the auto-login parameter was specified.

If no SSH authentication method is enabled, remote SSH clients must still be AAA-authenticated before being granted management access to the device.

If the auto-login keyword is specified for SSH authentication by public key management access is granted if SSH authentication succeeds and the name of SSH used is found in the local user database. The device management AAA authentication is transparent to the user. If the user name is not in the local user database, then the user receives a warning message, and the user will need to pass the device management AAA authentication independently of the SSH authentication.

if the auto-login keyword is not specified, management access is granted only if the user engages and passes both SSH authentication and device management AAA authentication independently.If no SSH authentication method is enabled management access is granted only if the user is AAA authenticated by the device management. No SSH authentication method means SSH is enabled and neither SSH authentication by public key nor password is enabled.

Example

The following example enables authentication of the SSH client.

```
switchxxxxxx(config)# ip ssh pubkey-auth
```

48.6. crypto key pubkey-chain ssh

The crypto key pubkey-chain ssh Global Configuration mode command enters the SSH Public Key-chain Configuration mode. This mode is used to manually specify device public keys, such as SSH client public keys.

Syntax

- crypto key pubkey-chain ssh

Default Configuration

Keys do not exist.

Command Mode

Global Configuration mode

User Guidelines

Use this command when you want to manually specify SSH client's public keys.

Example

The following example enters the SSH Public Key-chain Configuration mode and manually configures the RSA key pair for SSH public key-chain to the user 'bob'.

```
switchxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxx(config-keychain)# user-key bob rsa
switchxxxxxx(config-keychain-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+ Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1g
kTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSq muSn/Wd05iDX2IExQWu08licglk02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+ Rmt5nhhqdAtN/4oJfce166DqVX1gWmN
zNR4DYDvSzg0lDnwCAC8Qh
Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

48.7. user-key

The `user-key` SSH Public Key-string Configuration mode command associates a username with a manually-configured SSH public key.

Use the no user-key command to remove an SSH user and the associated public key.

Syntax

- user-key username {rsa | dsa}
- no user-key username

Parameters

- username - Specifies the remote SSH client username. (Length: 1–48 characters)
- rsa - Specifies that the RSA key pair is manually configured.
- dsa - Specifies that the DSA key pair is manually configured.

Default Configuration

No SSH public keys exist.

Command Mode

SSH Public Key-string Configuration mode

User Guidelines

After entering this command, the existing key, if any, associated with the user will be deleted. You must follow this command with the key-string command to configure the key to the user.

Example

The following example enables manually configuring an SSH public key for SSH public key-chain bob.

```
switchxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxx(config-keychain)# user-key bob rsa
switchxxxxxx(config-keychain-key)# key-string row
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
```

48.8. key-string

The key-string SSH Public Key-string Configuration mode command manually specifies an SSH public key.

Syntax

- key-string [row key-string]

Parameters

- row - Specifies the SSH public key row by row. The maximum length of a row is 160 characters.
- key-string - Specifies the key in UU-encoded DER format. UU-encoded

DER format is the same format as in the authorized_keys file used by OpenSSH.

Default Configuration

Keys do not exist.

Command Mode

SSH Public Key-string Configuration mode

User Guidelines

Use the key-string SSH Public Key-string Configuration mode command without the row parameter to specify which SSH public key is to be interactively configured next. Enter a row with no characters to complete the command.

Use the key-string row SSH Public Key-string Configuration mode command to specify the SSH public key, row by row. Each row must begin with a key-string row command.

The UU-encoded DER format is the same format as in the authorized_keys file used by OpenSSH.

Example

The following example enters public key strings for SSH public key client 'bob'.

```
switchxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxx(config-keychain)# user-key bob rsa
switchxxxxxx(config-keychain-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+ Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1g
kTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSq muSn/Wd05iDX2IExQWu08licglk02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+ Rmt5nhhqdAtN/4oJfce166DqVX1gWmN
zNR4DYDvSzg0lDnwCAC8Qh
Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
switchxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxx(config-keychain)# user-key bob rsa
switchxxxxxx(config-keychain-key)# key-string row AAAAB3Nza
switchxxxxxx(config-keychain-key)# key-string row C1yc2
```

48.9. show ip ssh

The show ip ssh Privileged EXEC mode command displays the SSH server configuration.

Syntax

- show ip ssh

Command Mode

Privileged EXEC mode

Example

The following example displays the SSH server configuration.

```
switchxxxxxx# show ip ssh
SSH server enabled. Port: 22 RSA key was generated.
DSA (DSS) key was generated. SSH Public Key Authentication is enabled with auto-
login.
SSH Password Authentication is enabled.
Active incoming sessions:
IP Address SSH Username Version Cipher Auth Code
---------- ------------ ------- ------ ---------
172.16.0.1 John Brown 1.5 3DES HMAC-SHA1
182.20.2.1 Bob Smith 1.5 3DES Password
```

The following table describes the significant fields shown in the display.

Field	Description
IP Address	The client address
SSH Username	The user name
Version	The SSH version number
Cipher	The encryption type (3DES, Blowfish, RC4)
Auth Code	The authentication Code (HMAC-MD5, HMAC-SHA1) or Password

48.10. show crypto key pubkey-chain ssh

The show crypto key pubkey-chain ssh Privileged EXEC mode command displays SSH public keys stored on the device.

Syntax

- show crypto key pubkey-chain ssh [username username] [fingerprint {bubble-babble | hex}]

Parameters

- username username - Specifies the remote SSH client username. (Length: 1–48 characters)
- fingerprint {bubble-babble | hex} - Specifies the fingerprint display format. The possible values are:
  - bubble-babble - Specifies that the fingerprint is displayed in Bubble Babble format.
  - hex - Specifies that the fingerprint is displayed in hexadecimal format.

Default Configuration

The default fingerprint format is hexadecimal.

Command Mode

Privileged EXEC mode

Example

The following examples display SSH public keys stored on the device.

```
switchxxxxxx# show crypto key pubkey-chain ssh
Username Fingerprint
---------- -----------------------------------------------------------bob
9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86 john
98:F7:6E:28:F2:79:87:C8:18:F8:88:CC:F8:89:87:C8
switchxxxxxx# show crypto key pubkey-chain ssh username bob
Username Fingerprint
---------- -----------------------------------------------------------bob
9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86
```

49. sFlow Commands

49.1. sflow receiver

To define the sFlow collector, use the `sflow receiver` Global Configuration mode command. To remove the definition of the collector, use the no form of this command.

Syntax

- sflow receiver index {ipv4-address | ipv6-address | hostname} [port port] [max-datagram-size bytes]
- no sflow receiver index

Parameters

- index - The index of the receiver. (Range: 1–8)
- ipv4-address - IPv4 address of the host to be used as an sFlow Collector.
- ipv6-address - IPv6 address of the host to be used as an sFlow Collector. When the IPv6 address is a Link Local address (IPv6 address), the outgoing interface name must be specified. Refer to the User Guidelines for the interface name syntax.
- hostname - Hostname of the host to be used as an sFlow Collector.
- port - (Optional) Port number for sflow messages. If unspecified, the port number defaults to 6343. The range is 1-65535.
- bytes - (Optional) Specifies the maximum datagramsize that can be sent. If unspecified, it defaults to 1400.

Default

No receiver is defined.

Command Mode

Global Configuration mode

User Guidelines

If the IP address of the sFlow receiver is set to 0.0.0.0, no sFlow datagrams are sent.

49.2. sflow flow-sampling

To enable sFlow Flow sampling and configure the average sampling rate of a specific port, use the `sflow flow-sampling` Interface Configuration mode command. To disable Flow sampling, use the no form of this command.

Syntax

- sflow flow-sampling rate receiver-index [max-header-size bytes]
- no sflow flow-sampling

Parameters

- rate - Specifies the average sampling rate. The sampling rate is calculated as 1/rate (Range: 1024–1073741823.)
- receiver-index - Index of the receiver/collector (Range: 1–8.)
- bytes - (Optional) Specifies the maximum number of bytes that would be copied from the sampled packet. If unspecified, defaults to 128. (Range: 20–256.)

Default

Disabled

Command Mode

Interface Configuration mode

User Guidelines

A new sampling rate configuration is not immediately loaded to the hardware. It will be loaded to the hardware only after the next packet is sampled (based on the current sampling rate).

49.3. sflow counters-sampling

To enable sFlow Counters sampling and to configure the maximum interval of a specific port, use the `sflow counters-sampling` Interface Configuration mode command . To disable sFlow Counters sampling, use the no form of this command.

Syntax

- sflow counters-sampling interval receiver-index
- no sflow counters-sampling

Parameters

- interval - Specifies the maximum number of seconds between successive samples of the interface counters. (Range: 15–86400.)
- receiver-index - Index of the receiver/collector. (Range: 1–8.)

Default

Disabled

Command Mode

Interface Configuration mode

49.4. clear sflow statistics

To clear sFlow statistics, use the `clear sFlow statistics` Privileged EXEC mode command.

Syntax

- clear sflow statistics [interface-id]

Parameters

- interface-id - (Optional) Specifies an interface ID. The interface ID must be an Ethernet port.

Command Mode

Privileged EXEC mode

User Guidelines

If no interface is specified by the user, the command clears all the sFlow statistics counters (including datagrams sent). If an interface is specified by the user, the command clears only the counter of the specific interface.

49.5. show sflow configuration

To display the sFlow configuration for ports that are enabled for Flow sampling or Counters sampling, use the `show sflow configuration` Privileged EXEC mode command.

Syntax

- show sflow configuration [interface-id]

Parameters

- interface-id - (Optional) Specifies an interface ID. The interface ID must be an Ethernet port.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show sflow configuration
Receivers
Index IP Address Port Max Datagram Size
----- ------------------- -------- ----------------
 1 0.0.0.0 6343 1400
 2 172.16.1.2 6343 1400
 3 0.0.0.0 6343 1400
 4 0.0.0.0 6343 1400
 5 0.0.0.0 6343 1400
 6 0.0.0.0 6343 1400
 7 0.0.0.0 6343 1400
 8 0.0.0.0 6343 1400

Interfaces
Inter- Flow Counters Max Header Flow Counters Collector face Sampling Sampling
Size Collector Index Index
 ----- ----------- --------- --------- ---------- ----- ------------
te1/0/1 1/2048 60 sec 128 1    1
te1/0/2 1/4096 Disabled 128 0        2

Global values
--------------
Source IPv4 interface: vlan 120
Source IPv6 interface: vlan 10
```

49.6. show sflow statistics

To display the sFlow statistics for ports that are enabled for Flow sampling or Counters sampling, use the `show sflow statistics` Privileged EXEC mode command.

Syntax

- show sflow statistics [interface-id]

Parameters

- interface-id - (Optional) Specifies an interface ID. The interface ID must be an Ethernet port.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show sflow statistics
Total sFlow datagrams sent to collectors: 100
```

```
Interface Packets sampled Datagrams sent to collector
--------- --------------- --------------
te1/0/1 30 50
te1/0/2 30 50
te1/0/3 30 50
```

49.7. sflow receiver source-interface

Use the `sflow receiver source-interface` Global Configuration mode command to specify the source interface whose IPv4 address will be used as the Source IPv4 address for communication with sFlow receivers. Use the no form of this command to restore the default configuration.

Syntax

- sflow receiver source-interface interface-id
- no sflow receiver source-interface

Parameters

- interface-id - Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the interface IP address belonging to next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface, the minimal IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 sFlow server.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# sflow receiver source-interface vlan 100
```

49.8. sflow receiver source-interface-ipv6

Use the `sflow receiver source-interface-ipv6` Global Configuration mode command to specify the source interface whose IPv6 address will be used as the source IPv6 address for communication with IPv6 sFlow receivers. Use the no form of this command to restore the default configuration.

Syntax

- sflow receiver source-interface-ipv6 interface-id
- no sflow receiver source-interface-ipv6

Parameters

- interface-id - Specifies the source interface.

Default Configuration

The IPv6 source address is the IPv6 address defined on the outgoing interface and selected in accordance with RFC6724.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the source IPv6 address is an IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

If the source interface is not the outgoing interface, the source IPv6 address is the minimal IPv6 address defined on the source interface and matched to the scope of the destination IPv6 address is applied.

If there is no available source IPv6 address, a SYSLOG message is issued when attempting to communicate with an IPv6 sFlow receiver.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# sflow receiver source-interface-ipv6 vlan 100
```

50. Network Management Protocol (SNMP) Commands

50.1. snmp-server community

To set the community access string (password) that permits access to SNMP commands (v1 and v2), use the `snmp-server community` Global Configuration mode command. This is used for SNMP commands, such as GETs and SETs.

This command configures both SNMP v1 and v2.

To remove the specified community string, use the no form of this command.

Syntax

- snmp-server community community-string [ro | rw | su] [ip-address | ipv6-address] [mask mask | prefix prefix-length] [view view-name] [type {router | oob}]
- no snmp-server community community-string [ip-address] [type {router | oob}]

Parameters

- community-string - Define the password that permits access to the SNMP protocol. (Range: 1–20 characters).
- ro - (Optional) Specifies read-only access (default)
- rw - (Optional) Specifies read-write access
- su - (Optional) Specifies SNMP administrator access
- ip-address - (Optional) Management station IP address. The default is all IP addresses. This can be an IPv4 address, IPv6 or IPv6 address. See `IPv6 Address Conventions`.
- mask - (Optional) Specifies the mask of the IPv4 address. This is not a network mask, but rather a mask that defines which bits of the packet's source address are compared to the configured IP address. If unspecified, it defaults to 255.255.255.255. The command returns an error if the mask is specified without an IPv4 address.
- prefix-length - (Optional) Specifies the number of bits that comprise the IPv4 address prefix. If unspecified, it defaults to 32. The command returns an error if the prefix-length is specified without an IPv4 address.
- view view-name - (Optional) Specifies the name of a view configured using the command `snmp-server view` (no specific order of the command configurations is imposed on the user). The view defines the objects available to the community. It is not relevant for su, which has access to the whole MIB. If unspecified, all the objects, except the community-table and SNMPv3 user and access tables , are available. (Range: 1–30 characters)
- type router - (Optional) Indicates whether the IP address is on the out-of-band or in-band network.

Default Configuration

No community is defined

Command Mode

Global Configuration mode

User Guidelines

It is possible to define up to 24 communities.

The logical key of the command is the pair (community, ip-address). If ip-address is omitted, the key is (community, All-IPs). This means that there cannot be two commands with the same community, ip address pair.

The view-name is used to restrict the access rights of a community string. When a view-name is specified, the software:

- Generates an internal security-name.
- Maps the internal security-name for SNMPv1 and SNMPv2 security models to an internal group-name.
- Maps the internal group-name for SNMPv1 and SNMPv2 security models to view-name (read-view and notify-view always, and for rw for write-view also),

Example

Defines a password for administrator access to the management station at IP address 1.1.1.121 and mask 255.0.0.0.

```
switchxxxxxx(config)# snmp-server community abcd su 1.1.1.121 mask 255.0.0.0
```

50.2. snmp-server community-group

To configure access rights to a user group, use snmp-server community-group. The group must exist in order to be able to specify the access rights. This command configures both SNMP v1 and v2.

Syntax

- snmp-server community-group community-string group-name [ip-address | ipv6-address] [mask mask | prefix prefix-length] [type {router | oob}]

Parameters

- community-string - Define the password that permits access to the SNMP protocol. (Range: 1–20 characters).
- group-name - This is the name of a group configured using `snmp-server group` with v1 or v2 (no specific order of the two command configurations is imposed on the user). The group defines the objects available to the community. (Range: 1–30 characters)
- ip-address - (Optional) Management station IP address. The default is all IP addresses. This can be an IPv4 address, IPv6 or IPv6 address. See `IPv6 Address Conventions`.
- mask - (Optional) Specifies the mask of the IPv4 address. This is not a network mask, but rather a mask that defines which bits of the packet's source address are compared to the configured IP address. If unspecified, it defaults to 255.255.255.255. The command returns an error if the mask is specified without an IPv4 address.
- prefix-length - (Optional) Specifies the number of bits that comprise the IPv4 address prefix. If unspecified, it defaults to 32. The command returns an error if the prefix-length is specified without an IPv4 address.
- type router - (Optional) Indicates whether the IP address is on the out-of-band or in-band network.

Default Configuration

No community is defined

Command Mode

Global Configuration mode

User Guidelines

The group-name is used to restrict the access rights of a community string. When a group-name is specified, the software:

- Generates an internal security-name.
- Maps the internal security-name for SNMPv1 and SNMPv2 security models to the group-name.

Example

Defines a password tom for the group abcd that enables this group to access the management station 1.1.1.121 with prefix 8.

```
switchxxxxxx(config)# snmp-server community-group tom abcd 1.1.1.122 prefix 8
```

50.3. snmp-server server

To enable the device to be configured by the SNMP protocol, use the `snmp-server server` Global Configuration mode command. To disable this function, use the no form of this command.

Syntax

- snmp-server server
- no snmp-server server

Parameters

This command has no arguments or keywords.

Default Configuration

Enabled

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# snmp-server server
```

50.4. snmp-server source-interface

To specify the interface from which a Simple Network Management Protocol (SNMP) trap originates the informs or traps, use the `snmp-server source-interface` command in Global Configuration mode. To returned to the default, use the no form of this command.

Syntax

- snmp-server source-interface {traps | informs} interface-id
- no snmp-server source-interface [traps | informs]

Parameters

- traps - Specifies the SNMP traps interface.
- informs - Specifies the SNMP informs.
- interface-id - Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

If no parameters are specified in no snmp-server source-interface, the default is both traps and informs.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the interface IP address belonging to next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface, the minimal IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to send an SNMP trap or inform.

Use the no snmp-server source-interface traps command to remove the source interface for SNMP traps.

Use the no snmp-server source-interface informs command to remove the source interface for SNMP informs.

Use the no snmp-server source-interface command to remove the source interface for SNMP traps and informs.

Example

The following example configures the VLAN 10 as the source interface for traps.

```
switchxxxxxx(config)# snmp-server source-interface traps vlan 100
```

50.5. snmp-server source-interface-ipv6

To specify the interface from which a Simple Network Management Protocol (SNMP) trap originates the informs or traps, use the `snmp-server source-interface-ipv6` command in Global Configuration mode. To returned to the default, use the no form of this command.

Syntax

- snmp-server source-interface-ipv6 {traps | informs} interface-id
- no snmp-server source-interface-ipv6 [traps | informs]

Parameters

- traps - Specifies the SNMP traps interface.
- informs - Specifies the SNMP traps informs.
- interface-id - Specifies the source interface.

Default Configuration

The IPv6 source address is the IPv6 address of the outgoing interface and selected in accordance with RFC6724.

If no parameters are specified in no snmp-server source-interface, the default is both traps and informs.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the IPv6 address defined on the interfaces is selected in accordance with RFC 6724.

If the source interface is not the outgoing interface, the minimal IPv6 address defined on the source interface with the scope of the destination IPv6 address is applied.

If there is no available IPv6 source address, a SYSLOG message is issued when attempting to send an SNMP trap or inform.

Use the no snmp-server source-interface-ipv6 traps command to remove the source IPv6 interface for SNMP traps.

Use the no snmp-server source-interface-ipv6 informs command to remove the source IPv6 interface for SNMP informs.

Use the no snmp-server source-interface-ipv6 command to remove the source IPv6 interface for SNMP traps and informs.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# snmp-server source-interface-ipv6 traps vlan 100
```

50.6. snmp-server view

To create or update an SNMP view, use the `snmp-server view` Global Configuration mode command. To remove an SNMP view, use the no form of this command.

Syntax

- snmp-server view view-name oid-tree {included | excluded}
- no snmp-server view view-name [oid-tree]

Parameters

- view-name - Specifies the name for the view that is being created or updated. (Length: 1–30 characters)
- included - Specifies that the view type is included.
- excluded - Specifies that the view type is excluded.
- oid-tree - (Optional) Specifies the ASN.1 subtree object identifier to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as System and, optionally, a sequence of numbers. Replace a single sub-identifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4. This parameter depends on the MIB being specified.

Default Configuration

The following views are created by default:

- Default - Contains all MIBs except for those that configure the SNMP parameters themselves.
- DefaultSuper - Contains all MIBs.

Command Mode

Global Configuration mode

User Guidelines

This command can be entered multiple times for the same view.

The command's logical key is the pair (view-name, oid-tree). Therefore there cannot be two commands with the same view-name and oid-tree.

The number of views is limited to 64.

Default and DefaultSuper views are reserved for internal software use and cannot be deleted or modified.

Example

The following example creates a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interface group (this format is specified on the parameters specified in ifEntry).

```
switchxxxxxx(config)# snmp-server view user-view system included
switchxxxxxx(config)# snmp-server view user-view system.7 excluded
switchxxxxxx(config)# snmp-server view user-view ifEntry.*.1 included
```

50.7. snmp-server group

To configure an SNMP group, use the `snmp-server group` Global Configuration mode command. Groups are used to map SNMP users to SNMP views. To remove an SNMP group, use the no form of this command.

Syntax

- snmp-server group groupname {v1 | v2 | v3 {noauth | auth | priv} [notify notifyview]} [read readview] [write writeview]
- no snmp-server group groupname {v1 | v2 | v3 [noauth | auth | priv]}

Parameters

- group groupname - Specifies the group name. (Length: 1–30 characters)
- v1 - Specifies the SNMP Version 1 security model.
- v2 - Specifies the SNMP Version 2 security model.
- v3 - Specifies the SNMP Version 3 security model.
- noauth - Specifies that no packet authentication will be performed. Applicable only to the SNMP version 3 security model.
- auth - Specifies that packet authentication without encryption will be performed. Applicable only to the SNMP version 3 security model.
- priv - Specifies that packet authentication with encryption will be performed. Applicable only to the SNMP version 3 security model. Note that creation of SNMPv3 users with both authentication and privacy must be done in the GUI. All other users may be created in the CLI.
- notify notifyview - (Optional) Specifies the view name that enables generating informs or a traps. An inform is a trap that requires acknowledgement. Applicable only to the SNMP version 3 security model. (Length: 1–32 characters)
- read readview - (Optional) Specifies the view name that enables viewing only. (Length: 1–32 characters)
- write writeview - (Optional) Specifies the view name that enables configuring the agent. (Length: 1–32 characters)

Default Configuration

No group entry exists.

If notifyview is not specified, the notify view is not defined.

If readview is not specified, all objects except for the community-table and SNMPv3 user and access tables are available for retrieval.

If writeview is not specified, the write view is not defined.

Command Mode

Global Configuration mode

User Guidelines

The group defined in this command is used in the `snmp-server user` command to map users to the group. These users are then automatically mapped to the views defined in this command.

The command logical key is (groupname, snmp-version, security-level). For snmp-version v1/v2 the security-level is always noauth.

Example

The following example attaches a group called user-group to SNMPv3, assigns the encrypted security level to the group, and limits the access rights of a view called user-view to read-only. User tom is then assigned to user-group. So that user tom has the rights assigned in user-view.

```
switchxxxxxx(config)# snmp-server group user-group v3 priv read user-view
switchxxxxxx(config)# snmp-server user tom user-group v3
```

50.8. show snmp views

To display SNMP views, use the `show snmp views` Privileged EXEC mode command.

Syntax

- show snmp views [viewname]

Parameters

- viewname - (Optional) Specifies the view name. (Length: 1–30 characters)

Default Configuration

If viewname is not specified, all views are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays the configured SNMP views.

```
switchxxxxxx# show snmp views
Name OID Tree Type
---- -------- ----
Default iso Included
Default snmpNotificationMIB Excluded
DefaultSuper iso Included
```

50.9. show snmp groups

To display the configured SNMP groups, use the `show snmp groups` Privileged EXEC mode command.

Syntax

- show snmp groups [groupname]

Parameters

- groupname - (Optional) Specifies the group name. (Length: 1–30 characters)

Default Configuration

Display all groups.

Command Mode

Privileged EXEC mode

Example

The following example displays the configured SNMP groups.:

```
switchxxxxxx# show snmp groups
Name Security Views
 Model Level Read Write Notify
---- ----- ----- ---- ----- ------
user-group V2 no_auth Default "" ""
managers-group V2 no_auth Default Default ""
```

The following table describes significant fields shown above.

Field		Description
Name		Group name.
Security	Model	SNMP model in use (v1, v2 or v3).
Security	Level	Packet security. Applicable to SNMP v3 security only
Views	Read	View name enabling viewing the agent contents. If unspecified, all objects except the community-table and SNMPv3 user and access tables are available.
	Write	View name enabling data entry and managing the agent contents.
	Notify	View name enabling specifying an inform or a trap.

50.10. snmp-server user

To configure a new SNMP Version user, use the `snmp-server user` Global Configuration mode command. To remove a user, use the no form of the command. To enter the authentication and privacy passwords in encrypted form (see SSD), use the encrypted form of this command.

Syntax

- snmp-server user username groupname {v1 | v2c | [remote host] v3[auth {md5 | sha} auth-password [priv priv-password]]}
- no snmp-server user username {v1 | v2c | [remote host] v3[auth {md5 | sha}

Parameters

- username - Define the name of the user on the host that connects to the agent. (Range: Up to 20 characters).
- groupname - The name of the group to which the user belongs. The group should be configured using the command `snmp-server group` with v1 or v2c parameters (no specific order of the 2 command configurations is imposed on the user). (Range: Up to 30 characters)
- v1 - Specifies that the user is a v1 user.
- v2c - Specifies that the user is a v2c user..
- v3 - Specifies that the user is a v3 user..
- remote host - (Optional) IP address (IPv4, IPv6 or IPv6) or host name of the remote SNMP host. See `IPv6 Address Conventions`.
- auth - (Optional) Specifies which authentication level is to be used.
- md5 - (Optional) Specifies the HMAC-MD5-96 authentication level.
- Sha - (Optional) Specifies the HMAC-SHA-96 authentication level.
- auth-password - (Optional) Specifies the authentication password. Range: Up to 32 characters.
- priv-password - (Optional) Specifies the privacy password (The encryption algorithm used is data encryption standard - DES). Range: Up to 64 characters.

Default Configuration

No group entry exists.

Command Mode

Global Configuration mode

User Guidelines

For SNMP v1 and v2, this command performs the same actions as snmp-server community-group, except that snmp-server community-group configures both v1 and v2 at the same time. With this command, you must perform it once for v1 and once for v2.

When you enter the show running-config command, you do not see a line for the SNMP user defined by this command. To see if this user has been added to the configuration, type the show snmp user command.

A local SNMP EngineID must be defined in order to add SNMPv3 users to the device (use the `snmp-server engineID remote` command). For remote hosts users a remote SNMP EngineID is also required (use the `snmp-server engineID remote` command).

Changing or removing the value of snmpEngineID deletes the SNMPv3 users' database.

The logical key of the command is username.

Configuring a remote host is required in order to send informs to that host, because an inform is a trap that requires acknowledgement. A configured remote host is also able to manage the device (besides getting the informs)

To configure a remote user, specify the IP address for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID, using the `snmp-server engineID remote` command. The remote agent's SNMP engine ID is needed when computing the authentication and privacy digests from the password. If the remote engine ID is not configured first, the configuration command fails.

Since the same group may be defined several times, each time with different version or different access level (noauth, auth or auth & priv), when defining a user it is not sufficient to specify the group name, rather you must specify group name, version and access level for complete determination of how to handle packets from this user.

Example

This example assigns user tom to group abcd using SNMP v1 and v2c. The default is assigned as the engineID. User tom is assigned to group abcd using SNMP v1 and v2c

```
switchxxxxxx(config)# snmp-server user tom acbd v1
switchxxxxxx(config)# snmp-server user tom acbd v2c
switchxxxxxx(config)# snmp-server user tom acbd v3
```

50.11. show snmp users

To display the configured SNMP users, use the `show snmp users` Privileged EXEC mode command.

Syntax

- show snmp users [username]

Parameters

username - (Optional) Specifies the user name. (Length: 1–30 characters)

Default Configuration

Display all users.

Command Mode

Privileged EXEC mode

Example

The following examples displays the configured SNMP users:

```
switchxxxxxx# show snmp users
User name :u1rem
 Group name :group1
 Authentication Algorithm : None
 Privacy Algorithm : None
 Remote :11223344556677
 Auth Password :
 Priv Password :
User name : qqq
 Group name : www
 Authentication Algorithm : MD5
 Privacy Algorithm : None
 Remote :
 Auth Password : helloworld1234567890987665
 Priv Password :
User name : hello
 Group name : world
 Authentication Algorithm : MD5
 Privacy Algorithm : DES
 Remote :
 Auth Password (encrypted): Z/tC3UF5j0pYfmXm8xeMvcIOQ6LQ4GOACCGYLRdAgOE6XQKTC
qMlrnpWuHraRlZj
```

```
 Priv Password (encrypted) : kN1ZHzSLo6WWxlkuZVzhLOo1gI5waaNf7Vq6yLBpJdS4N68tL
 1tbTRSz2H4c4Q4o
User name : u1noAuth
 Group name : group1 Authentication Algorithm : None Privacy Algorithm : None
 Remote :
 Auth Password (encrypted) :
 Priv Password (encrypted) :
User name : u1OnlyAuth
 Group name : group1
 Authentication Algorithm : SHA
 Privacy Algorithm : None
 Remote :
 Auth Password (encrypted): 8nPzy2hzuba9pG3iiC/q0451RynUn7kq94L9WORFrRM= Priv
Password (encrypted) :
```

50.12. snmp-server host

To configure the host for SNMP notifications: (traps/informs), use the `snmp-server host` Global Configuration mode command. To remove the specified host, use the no form of this command.

Syntax

- snmp-server host {host-ip | hostname} [traps | informs] [version {1 | 2c | 3 [auth|noauth | priv]}] community-string [udp-port port][timeout seconds] [retries retries]
- no snmp-server host {ip-address | hostname} [traps | informs] [version {1 | 2c | 3}]

Parameters

- host-ip - IP address of the host (the targeted recipient). The default is all IP addresses. This can be an IPv4 address, IPv6 or IPv6 address. See `IPv6 Address Conventions`.
- hostname - Hostname of the host (the targeted recipient). (Range: 1–158 characters. Maximum label size of each part of the host name: 63)
- trap - (Optional) Sends SNMP traps to this host (default).
- informs - (Optional) Sends SNMP informs to this host. An inform is a trap that requires acknowledgement. Not applicable to SNMPv1.
- version 1 - (Optional) SNMPv1 traps are used.
- version 2c - (Optional) SNMPv2 traps or informs are used
- version 3 - (Optional) SNMPv2 traps or informs are used
- Authentication options are available for SNMP v3 only. The following options are available:
  - noauth - (Optional) Specifies no authentication of a packet.
  - auth - (Optional) Specifies authentication of a packet without encryption.
  - priv - (Optional) Specifies authentication of a packet with encryption.
- community-string - Password-like community string sent with the notification operation. (Range: 1–20 characters). For v1 and v2, any community string can be entered here. For v3, the community string must match the user name defined in snmp-server user (ISCLI) command for v3.
- udp-port port - (Optional) UDP port of the host to use. The default is 162. (Range: 1–65535)
- timeout seconds - (Optional) (For informs only) Number of seconds to wait for an acknowledgment before resending informs. The default is 15 seconds. (Range: 1–300)

- retries retries - (Optional) (For informs only) Maximum number of times to resend an inform request, when a response is not received for a generated message. The default is 3. (Range: 0–255)

Default Configuration

Version: SNMP V1

Type of notification: Traps udp-port: 162

If informs are specified, the default for retries: 3

Timeout: 15

Command Mode

Global Configuration mode

User Guidelines

It is possible to handle up to 24 notification recipients.

The logical key of the command is the list (ip-address/hostname, traps/informs, version).

When configuring SNMP v1 or v2 notifications recipient, the software automatically generates a notification view for that recipient for all MIBs.

For SNMPv3 the software does not automatically create a user or a notify view.

Use the commands snmp-server user (ISCLI) and snmp-server group to create a user or a group.

Example

The following defines a host at the IP address displayed.

```
switchxxxxxx(config)# snmp-server host 1.1.1.121 abc
```

50.13. snmp-server engineID local

To specify the SNMP engineID on the local device for SNMP v3, use the `snmp-server engineID local` Global Configuration mode command. To remove this engine ID, use the no form of this command.

Syntax

- snmp-server engineID local {engineid-string | default}
- no snmp-server engineID local

Parameters

- engineid-string - Specifies a concatenated hexadecimal character string identifying the engine ID. Each byte in a hexadecimal character string is two hexadecimal digits. Bytes are separated by a period or colon. If an odd number of hexadecimal digits are entered, the system automatically prefixes the digit 0 to the string. (Length: 5–32 characters, 9–64 hexadecimal digits)
- default - Specifies that the engine ID is created automatically based on the device MAC address.

Default Configuration

The default engine ID is defined per standard as:

- First 4 octets: First bit = 1, the rest is IANA Enterprise number = 674.

- Fifth octet: Set to 3 to indicate the MAC address that follows.
- Last 6 octets: The device MAC address.

Command Mode

Global Configuration mode

User Guidelines

To use SNMPv3, an engine ID must be specified for the device. Any ID can be specified or the default string, which is generated using the device MAC address, can be used.

As the engineID should be unique within an administrative domain, the following guidelines are recommended:

- Since the engineID should be unique within an administrative domain, use the default keyword to configure the Engine ID or configure it explicitly. In the latter case verify that it is unique within the administrative domain.
- Changing or removing the value of snmpEngineID deletes the SNMPv3 users database.
- The SNMP EngineID cannot be all 0x0 or all 0xF or 0x000000001.

Example

The following example enables SNMPv3 on the device and sets the device local engine ID to the default value.

```
switchxxxxxx(config)# snmp-server engineid local default
The engine-id must be unique within your administrative domain.
Do you wish to continue? [Y/N]Y
The SNMPv3 database will be erased. Do you wish to continue? [Y/N]Y
```

50.14. snmp-server engineID remote

To specify the SNMP engine ID of a remote SNMP device, use the `snmp-server engineID remote` Global Configuration mode command. To remove the configured engine ID, use the no form of this command.

Syntax

- snmp-server engineID remote ip-address engineid-string
- no snmp-server engineID remote ip-address

Parameters

- ip-address - IPv4, IPv6 or IPv6 address of the remote device. See `IPv6 Address Conventions`.
- engineid-string - The character string that identifies the engine ID. The engine ID is a concatenated hexadecimal string. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon. If the user enters an odd number of hexadecimal digits, the system automatically prefixes the hexadecimal string with a zero. (Range: engineid-string5–32 characters. 9–64 hexadecimal digits)

Default Configuration

The remote engineID is not configured by default.

Command Mode

Global Configuration mode

User Guidelines

A remote engine ID is required when an SNMP version 3 inform is configured. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

Example

```
switchxxxxxx(config)# snmp-server engineID remote 1.1.1.1 11:AB:01:CD:23:44
```

50.15. show snmp engineID

To display the local SNMP engine ID, use the `show snmp engineID` Privileged EXEC mode command.

Syntax

- show snmp engineID

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example displays the SNMP engine ID.

```
switchxxxxxx# show snmp engineID
Local SNMP engineID: 08009009020C0B099C075878
      IP address  Remote SNMP engineID
      ----------- ------------------------------
      172.16.08009009020C0B099C075879
```

50.16. snmp-server enable traps

To enable the device to send SNMP traps, use the `snmp-server enable traps` Global Configuration mode command. To disable all SNMP traps, use the no form of the command.

Syntax

- snmp-server enable traps
- no snmp-server enable traps

Default Configuration

SNMP traps are enabled.

Command Mode

Global Configuration mode

User Guidelines

If no snmp-server enable traps has been entered, you can enable failure traps by using `snmp-server trap authentication` as shown in the example.

Example

The following example enables SNMP traps except for SNMP failure traps.

```
switchxxxxxx(config)# snmp-server enable traps
switchxxxxxx(config)# no snmp-server trap authentication
```

50.17. snmp-server trap authentication

To enable the device to send SNMP traps when authentication fails, use the `snmp-server trap authentication` Global Configuration mode command. To disable SNMP failed authentication traps, use the no form of this command.

Syntax

- snmp-server trap authentication
- no snmp-server trap authentication

Parameters

This command has no arguments or keywords.

Default Configuration

SNMP failed authentication traps are enabled.

Command Mode

Global Configuration mode

User Guidelines

The command `snmp-server enable traps` enables all traps including failure traps. Therefore, if that command is enabled (it is enabled by default), this command is not necessary.

Example

The following example disables all SNMP traps and enables only failed authentication traps.

```
switchxxxxxx(config)# no snmp-server enable traps
switchxxxxxx(config)# snmp-server trap authentication
```

50.18. snmp-server contact

To set the value of the system contact (sysContact) string, use the `snmp-server contact` Global Configuration mode command. To remove the system contact information, use the no form of the command.

Syntax

- snmp-server contact text
- no snmp-server contact

Parameters

- text - Specifies system contact information. (Length: 1–160 characters)

Default Configuration

None

Command Mode

Global Configuration mode

Example

The following example sets the system contact information to Technical_Support.

```
switchxxxxxx(config)# snmp-server contact Technical_Support
```

50.19. snmp-server location

To set the value of the system location string, use the `snmp-server location` Global Configuration mode command. To remove the location string, use the no form of this command.

Syntax

- snmp-server location text
- no snmp-server location

Parameters

- text - Specifies the system location information. (Length: 1–160 characters)

Default Configuration

None

Command Mode

Global Configuration mode

Example

The following example sets the device location to New_York.

```
switchxxxxxx(config)# snmp-server location New_York
```

50.20. snmp-server set

To define SNMP MIB commands in the configuration file if a MIB performs an action for which there is no corresponding CLI command, use the `snmp-server set` Global Configuration mode command.

Syntax

- snmp-server set variable-name name value [name2 value2...]

Parameters

- variable-name - Specifies an SNMP MIB variable name, which must be a valid string.
- name value - Specifies a list of names and value pairs. Each name and value must be a valid string. In the case of scalar MIBs, there is only a single name-value pair. In the case of an entry in a table, there is at least one name-value pair, followed by one or more fields.

Default Configuration

None

Command Mode

Global Configuration mode

User Guidelines

Although the CLI can set any required configuration, there might be a situation where an SNMP user sets a MIB variable that does not have an equivalent CLI command. To generate configuration files that support those situations, the system uses `snmp-server set`. This command is not intended for the end user.

Example

The following example configures the scalar MIB sysName with the value TechSupp.

```
switchxxxxxx(config)# snmp-server set sysName sysname TechSupp
```

50.21. snmp trap link-status

To enable link-status generation of SNMP traps, use the `snmp trap link-status` Interface Configuration mode command. To disable generation of link-status SNMP traps, use the no form of this command.

Syntax

- snmp trap link-status
- no snmp trap link-status

Parameters

This command has no arguments or keywords.

Default Configuration

Generation of SNMP link-status traps is enabled

Command Mode

Interface Configuration mode

Example

The following example disables generation of SNMP link-status traps.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# # no snmp trap link-status
```

50.22. show snmp

To display the SNMP status, use the `show snmp` Privileged EXEC mode command.

Syntax

- show snmp

Parameters

This command has no arguments or keywords

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example displays the SNMP communications status.

```
switchxxxxxx# show snmp
SNMP is enabled
SNMP traps Source IPv4 interface: vlan 1
SNMP informs Source IPv4 interface: vlan 11
SNMP traps Source IPv6 interface: vlan 10 SNMP informs Source IPv6 interface:
Community-String Community-Access View name IP Address Mask ---------------- ---
------------ ------------ ---------- ----
public read only user-view All private read write Default 172.16.1.1/10 private
su DefaultSuper 172.16.1.1
Community-string  Group name  IP Address  Mask  Type ----------------   --------
--    ----------  -----public user-group  All   Router
Traps are enabled.
Authentication trap is enabled.
Version 1,2 notifications
      Target Address    Type  Community   Version     UDP   TO    Retries
      Port  Sec
      ----------- ----  --------    -------     ----  ---   -------
      192.122.17Trap    public      2     162   15    3
      192.122.17Inform  public      2     162   15    3
Version 3 notifications
Target Address Type Username Security UDP TO Retries
  Level Port Sec
-------------- ------ -------- -------- ---- --- -------
192.122.173.42 Inform Bob Priv 162 15 3
System Contact: Robert
System Location: Marketing
```

The following table describes the significant fields shown in the display.

Field	Description
Community-string	The community access string permitting access to SNMP.
Community-access	The permitted access type - read-only, read-write, super access.
IP Address	The management station IP Address.
Target Address	The IP address of the targeted recipient.
Version	The SNMP version for the sent trap.

51. SPAN Commands

51.1. monitor session destination

To create a new Switched Port Analyzer (SPAN) destination session, use the `monitor session destination` command in Global Configuration mode. To remove a destination session, use the no form of the command.

Syntax

- monitor session session_number destination interface interface-id [network]
- no monitor session session_number destination

Parameters

- session_number - Specify the session number identified with the SPAN or flow mirror session. The range is 1 to 7.
- interface interface-id - Specify the destination interface for the SPAN or flow mirror session (Ethernet port).
- network - Specify that the destination port acts also as a network port.

Default Configuration

No SPAN sessions are configured.

Command Mode

Global Configuration mode

User Guidelines

Use the monitor session session_number destination interface interface-id, to create a SPAN or flow mirror destination session to copy traffic to a destination port.

A destination port cannot be a source port.

A destination port cannot be a OOB port.

If the network keyword is not defined only mirrored traffic sent on a destination port and all input traffic is discard and a value of DOWN is advertised as its operational status to all applications running on it.

A destination port configured without the network keyword has the following limitations:

- 802.1x cannot be enabled on the port.

A port cannot be configured as destination port with the network keyword if it belongs to the source VLAN.

Please, do not add the destination port to the source VLAN.

Mirrored traffic is sent to queue number 1 of the destination port.

Use the no monitor session session_number destination command to remove one destination session.

Example

Example 1. The following example configures a SPAN session consisting from 3 source and one destination session. The first source session copies traffic for both directions from the source port `te1/0/`2, the second source session copies bridges traffic from VLAN 100, and the third source session copies traffic for received on the source port `te1/0/`3. The destination session defines port `te1/0/1 as the destination port`.

```
switchxxxxxx(config)# monitor session 1 source interface te1/0/2 both
switchxxxxxx(config)# monitor session 1 source vlan 100
switchxxxxxx(config)# monitor session 1 source interface te1/0/3 rx
switchxxxxxx(config)# monitor session 1 destination interface te1/0/1
```

Example 2. The following example configures a flow mirror session:

```
switchxxxxxx(config)# ip access-list extended ip1
switchxxxxxx(config-ip-al)# permit ip any any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# class-map c1
switchxxxxxx(config-cmap)# match access-group ip1
switchxxxxxx(config-cmap)# exit
switchxxxxxx(config)# policy-map p1
switchxxxxxx(config-pmap)# class c1
switchxxxxxx(config-pmap-c)# mirror 1
switchxxxxxx(config-pmap-c)# exit
switchxxxxxx(config-pmap)# exit
```

51.2. monitor session source

To create a new Switched Port Analyzer (SPAN) source session, use the `monitor session source` command in Global Configuration mode. To remove a source session, use the no form of the command.

Syntax

- monitor session session_number source {interface interface-id [both | rx | tx]} | {vlan vlan-id}
- no monitor session session_number source [{interface interface-id} | {vlan vlan-id}]

Parameters

- session_number - Specify the session number identified with the SPAN session. The range is 1 to 7.
- interface interface-id - Specify the source interface for a SPAN session (Ethernet port).
- both, rx, tx - Specify the traffic direction to monitor. If you do not specify a traffic direction, the source interface sends both transmitted and received traffic.
- vlan vlan-id - Specify the SPAN source interface as a VLAN ID. In this case only a value of 1 is allowed for the session_number argument.

Default Configuration

No SPAN sessions are configured.

Command Mode

Global Configuration mode

User Guidelines

Use the monitor session session_number source interface interface-id [both | rx | tx] command, to create a SPAN start source session to monitor traffic that enters or leaves a source port.

Use the monitor session session_number source vlan vlan-id command, to create a SPAN source session to monitor traffic that bridged into a source VLAN.

A SPAN session consists from up to 8 sources and one destination with the same session number.

Each monitor session source command defines one source port or VLAN. Different monitor session source commands must define different sources. A new command with the same session number and the same source overrides the previous defined one.

Up to 8 sources can be defined in one session.

If a packet is mirrored by both the port-based ingress mirroring mechanism, and one of the other ingress mirroring mechanisms, the selected session is the one with the higher session number.

All definitions of different source ports for the same source session must be of the same type: SPAN.

A source port cannot be a destination port.

A source port cannot be the a OOB port.

Use the no monitor session session_number source {interface interface-id} | {vlan vlan-id} command to remove one source.

Use the no monitor session session_number source command to remove all sources ports of the given source session.

Example

Example. The following example configures a SPAN session consisting from 3 source and one destination session. The first source session copies traffic for both directions from the source port `te1/0/2`, the second source session copies bridges traffic from VLAN 100, and the third source session copies traffic for received on the source port `te1/0/3`. The destination session defines port `te1/0/1 as the destination port.`

```
switchxxxxxx(config)# monitor session 1 source interface te1/0/2 both
switchxxxxxx(config)# monitor session 1 source vlan 100
switchxxxxxx(config)# monitor session 1 source interface te1/0/3 rx
switchxxxxxx(config)# monitor session 1 destination interface te1/0/1
```

51.3. show monitor session

To display information about Switched Port Analyzer (SPAN) sessions on the switch, use the `show monitor session` command in User EXEC mode.

Syntax

- show monitor session [session_number]

Parameters

- session_number - Specify the session number identified with the SPAN session. The range is 1 to 7. If the argument is not defined information about all sessions are displayed.

Default Configuration

This command has no default settings.

Command Mode

User EXEC mode

User Guidelines

Use the show monitor session session_number command to display information about one session.

Use the show monitor session command to display information about all sessions

Example

Example. The following example displays information about all SPAN sessions defined into the switch:

```
switchxxxxxx> show monitor session
Session 1
 Type: SPAN
 Source: te1/0/2, rx only
 Source: VLAN 100
 Source: flow mirrow, policy-map: alpha class-maps: ip-http, ipv6-http
 Destination: te1/0/1, network port
Field Definitions:
Type - The type of the session.
Source - A source of the session. The following options are supported:
Source: interface-id, traffic-direction(rx only,tx only, or both)
 The Source is an interface.
Source: vlan vlan-id
 The Source is a VLAN.
Source: flow mirrow, policy-map: policy-map-name, class-maps: class-map-name1,
class-map-name2
 The Source is a flow mirror, only attached policy-names are displayed.
Destination - A destination of the session. The following options are supported:
Destination: interface-id
 The Destination is an interface, regular forwarding on the interface is not
supported.
Destination: interface-id, network
 The Destination is an interface, regular forwarding on the interface is
supported.
```

52. Spanning-Tree Commands

52.1. spanning-tree

Use the `spanning-tree` Global Configuration mode command to enable spanning-tree functionality. Use the no form of this command to disable the spanning-tree functionality.

Syntax

- spanning-tree
- no spanning-tree

Parameters

N/A

Default Configuration

Spanning-tree is enabled.

Command Mode

Global Configuration mode

Example

The following example enables spanning-tree functionality.

```
switchxxxxxx(config)# spanning-tree
```

52.2. spanning-tree mode

Use the `spanning-tree mode` Global Configuration mode command to select which Spanning Tree Protocol (STP) protocol to run. Use the no form of this command to restore the default configuration.

Syntax

- spanning-tree mode {stp| rstp | mst}
- no spanning-tree mode

Parameters

- stp - Specifies that STP is enabled.
- rstp - Specifies that the Rapid STP is enabled.
- mst - Specifies that the Multiple STP is enabled.

Default Configuration

The default is `RSTP`.

Command Mode

Global Configuration mode

User Guidelines

In RSTP mode, the device uses STP when the neighbor device uses STP.

In MSTP mode, the device uses RSTP when the neighbor device uses RSTP, and uses STP when the neighbor device uses STP.

Example

The following example enables MSTP.

```
switchxxxxxx(config)# spanning-tree mode mst
```

52.3. spanning-tree forward-time

Use the `spanning-tree forward-time` Global Configuration mode command to configure the spanning-tree bridge forward time, which is the amount of time a port remains in the listening and learning states before entering the forwarding state. Use the no form of this command to restore the default configuration.

Syntax

- spanning-tree forward-time seconds
- no spanning-tree forward-time

Parameters

- seconds - Specifies the spanning-tree forward time in seconds. (Range: 4–30)

Default Configuration

15 seconds.

Command Mode

Global Configuration mode

User Guidelines

When configuring the forwarding time, the following relationship should be maintained:

2*(Forward-Time - 1) >= Max-Age

Example

The following example configures the spanning tree bridge forwarding time to 25 seconds.

```
switchxxxxxx(config)# spanning-tree forward-time 25
```

52.4. spanning-tree hello-time

Use the `spanning-tree hello-time` Global Configuration mode command to configure how often the device broadcasts Hello messages to other devices. Use the no form of this command to restore the default configuration.

Syntax

- spanning-tree hello-time seconds
- no spanning-tree hello-time

Parameters

- seconds - Specifies the spanning-tree Hello time in seconds. (Range: 1–10)

Default Configuration

2 seconds.

Command Mode

Global Configuration mode

User Guidelines

When configuring the Hello time, the following relationship should be maintained:

Max-Age >= 2*(Hello-Time + 1)

Example

The following example configures the spanning-tree bridge hello time to 5 seconds.

```
switchxxxxxx(config)# spanning-tree hello-time 5
```

52.5. spanning-tree max-age

Use the `spanning-tree max-age` Global Configuration mode command to configure the STP maximum age. Use the no form of this command to restore the default configuration.

Syntax

- spanning-tree max-age seconds
- no spanning-tree max-age

Parameters

- seconds - Specifies the spanning-tree bridge maximum age in seconds. (Range: 6–40)

Default Configuration

The default maximum age is 20 seconds.

Command Mode

Global Configuration mode

User Guidelines

When configuring the maximum age, the following relationships should be maintained:

2*(Forward-Time - 1) >= Max-Age

Max-Age >= 2*(Hello-Time + 1)

Example

The following example configures the spanning-tree bridge maximum age to 10 seconds.

```
switchxxxxxx(config)# spanning-tree max-age 10
```

52.6. spanning-tree priority

Use the `spanning-tree priority` Global Configuration mode command to configure the device STP priority, which is used to determine which bridge is selected as the root bridge. Use the no form of this command to restore the default device spanning-tree priority.

Syntax

- spanning-tree priority priority
- no spanning-tree priority

Parameters

- priority - Specifies the bridge priority. (Range: 0–61440)

Default Configuration

Default priority = 32768.

Command Mode

Global Configuration mode

User Guidelines

The priority value must be a multiple of 4096.

The switch with the lowest priority is the root of the spanning tree. When more than one switch has the lowest priority, the switch with the lowest MAC address is selected as the root.

Example

The following example configures the spanning-tree priority to 12288.

```
switchxxxxxx(config)# spanning-tree priority 12288
```

52.7. spanning-tree disable

Use the `spanning-tree disable` Interface (Ethernet, Port Channel) Configuration mode command to disable the spanning tree on a specific port. Use the no form of this command to enable the spanning tree on a port.

Syntax

- spanning-tree disable
- no spanning-tree disable

Parameters

N/A

Default Configuration

Spanning tree is enabled on all ports.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example disables the spanning tree on `te1/0/5`

```
switchxxxxxx(config)# interface te1/0/5
switchxxxxxx(config-if)# spanning-tree disable
```

52.8. spanning-tree cost

Use the `spanning-tree cost` Interface (Ethernet, Port Channel) Configuration mode command to configure the spanning-tree path cost for a port. Use the no form of this command to restore the default configuration.

Syntax

- spanning-tree cost cost
- no spanning-tree cost

Parameters

- cost - Specifies the port path cost. (Range: 1–200000000)

Default Configuration

Default path cost is determined by port speed and path cost method (long or short)as shown below

Interface	Long	Short
Port-channel	Half the default cost based on Port-channel interface speed	Half the default cost based on Port-channel interface speed
TenGigabit Ethernet (10000 Mbps)	2000	2
Gigabit Ethernet (1000 Mbps)	20,000	4
Fast Ethernet (100 Mbps)	200,000	19
Ethernet (10 Mbps)	2,000,000	100

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example configures the spanning-tree cost on `te1/0/`15 to 35000.

```
switchxxxxxx(config)# interface te1/0/15
switchxxxxxx(config-if)# spanning-tree cost 35000
```

52.9. spanning-tree port-priority

Use the `spanning-tree port-priority` Interface (Ethernet, Port Channel)

Configuration mode command to configure the port priority. Use the no form of this command to restore the default configuration.

Syntax

- spanning-tree port-priority priority
- no spanning-tree port-priority

Parameters

- priority - Specifies the port priority. (Range: 0–240)

Default Configuration

The default port priority is 128.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The priority value must be a multiple of 16.

Example

The following example configures the spanning priority on `te1/0/`15 to 96

```
switchxxxxxx(config)# interface te1/0/15
switchxxxxxx(config-if)# spanning-tree port-priority 96
```

52.10. spanning-tree portfast

Use the `spanning-tree portfast` Interface (Ethernet, Port Channel) Configuration mode command to enable the PortFast mode. In PortFast mode, the interface is immediately put into the forwarding state upon linkup, without waiting for the standard forward time delay. Use the no form of this command to disable the PortFast mode.

Syntax

- spanning-tree portfast [auto]
- no spanning-tree portfast

Parameters

- auto - Specifies that the software waits for 3 seconds (with no Bridge Protocol Data Units (BPDUs) received on the interface) before putting the interface into the PortFast mode.

Default Configuration

PortFast mode is disabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example enables the PortFast mode on `te1/0/`15.

```
switchxxxxxx(config)# interface te1/0/15
switchxxxxxx(config-if)# spanning-tree portfast
```

52.11. spanning-tree link-type

Use the `spanning-tree link-type` Interface (Ethernet, Port Channel) Configuration mode command to override the default link-type setting determined by the port duplex mode, and enable RSTP transitions to the Forwarding state. Use the no form of this command to restore the default configuration.

Syntax

- spanning-tree link-type {point-to-point | shared}
- no spanning-tree spanning-tree link-type

Parameters

- point-to-point - Specifies that the port link type is point-to-point.
- shared - Specifies that the port link type is shared.

Default Configuration

The device derives the port link type from the duplex mode. A full-duplex port is considered a point-to-point link and a half-duplex port is considered a shared link.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

The following example enables shared spanning-tree on `te1/0/1`5.

```
switchxxxxxx(config)# interface te1/0/15
switchxxxxxx(config-if)# spanning-tree link-type shared
```

52.12. spanning-tree pathcost method

Use the `spanning-tree pathcost method` Global Configuration mode command to set the default path cost method. Use the no form of this command to return to the default configuration.

Syntax

- spanning-tree pathcost method {long | short}
- no spanning-tree pathcost method

Parameters

- long - Specifies that the default port path costs are within the range: 1– 200,000,000.
- short - Specifies that the default port path costs are within the range: 1– 65,535.

Default Configuration

Long path cost method.

Command Mode

Global Configuration mode

User Guidelines

- This command applies to all the spanning tree instances on the switch. If the short method is selected, the switch calculates the default cost as 100.
- If the long method is selected, the switch calculates the default cost as 20000.

The following example sets the default path cost method to Long.

```
switchxxxxxx(config)# spanning-tree pathcost method long
```

52.13. spanning-tree bpdu (Global)

Use the `spanning-tree bpdu` Global Configuration mode command to define Bridge Protocol Data Unit (BPDU) handling when the spanning tree is disabled globally or on a single interface. Use the no form of this command to restore the default configuration.

Syntax

- spanning-tree bpdu {filtering | flooding}
- no spanning-tree bpdu

Parameters

- filtering - Specifies that BPDU packets are filtered when the spanning tree is disabled on an interface.
- flooding - Specifies that untagged BPDU packets are flooded unconditionally (without applying VLAN rules) to all ports with the spanning tree disabled and BPDU handling mode of flooding. Tagged BPDU packets are filtered.

Default Configuration

The default setting is flooding.

Command Mode

Global Configuration mode

User Guidelines

The filtering and flooding modes are relevant when the spanning tree is disabled globally or on a single interface.

The following example defines the BPDU packet handling mode as flooding when the spanning tree is disabled on an interface.

```
switchxxxxxx(config)# spanning-tree bpdu flooding
```

52.14. spanning-tree bpdu (Interface)

Use the `spanning-tree bpdu` Interface (Ethernet, Port Channel) Configuration mode command to define BPDU handling when the spanning tree is disabled on a single interface. Use the no form of this command to restore the default configuration.

Syntax

- spanning-tree bpdu {filtering | flooding}
- no spanning-tree bpdu

Parameters

- filtering - Specifies that BPDU packets are filtered when the spanning tree is disabled on an interface.
- flooding - Specifies that untagged BPDU packets are flooded unconditionally (without applying VLAN rules) to ports with the spanning tree disabled and BPDU handling mode of flooding. Tagged BPDU packets are filtered.

Default Configuration

The `spanning-tree bpdu (Global)` command determines the default configuration.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example defines the BPDU packet as flooding when the spanning tree is disabled on `te1/0/3`.

```
switchxxxxxx(config)# interface te1/0/3
switchxxxxxx(config-if)# spanning-tree bpdu flooding
```

52.15. spanning-tree guard root

use the `spanning-tree guard root` Interface (Ethernet, Port Channel) Configuration mode command to enable Root Guard on all spanning-tree instances on the interface. Root guard prevents the interface from becoming the root port of the device. Use the no form of this command to disable the root guard on the interface.

Syntax

- spanning-tree guard root
- no spanning-tree guard root

Default Configuration

Root guard is disabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Root Guard can be enabled when the device operates in any mode (STP, RSTP and MSTP).

When Root Guard is enabled, the port changes to the alternate state if the spanning-tree calculations select the port as the root port.

Example

The following example prevents `te1/0/1` from being the root port of the device.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# spanning-tree guard root
```

52.16. spanning-tree bpduguard

Use the `spanning-tree bpduguard` Interface (Ethernet, Port Channel) Configuration mode command to shut down an interface when it receives a Bridge Protocol Data Unit (BPDU). Use the no form of this command to restore the default configuration.

Syntax

- spanning-tree bpduguard {enable | disable}
- no spanning-tree bpduguard

Parameters

- enable - Enables BPDU Guard.
- disable - Disables BPDU Guard.

Default Configuration

BPDU Guard is disabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The command can be enabled when the spanning tree is enabled (useful when the port is in the PortFast mode) or disabled.

Example

The following example shuts down `te1/0/5` when it receives a BPDU.

```
switchxxxxxx(config)# interface te1/0/5
switchxxxxxx(config-if)# spanning-tree bpduguard enable
```

52.17. clear spanning-tree detected-protocols

Use the `clear spanning-tree detected-protocols` Privileged EXEC mode command to restart the STP migration process (force renegotiation with neighboring switches) on all interfaces or on the specified interface

Syntax

- clear spanning-tree detected-protocols [interface interface-id]

Parameters

- interface-id - Specifies an interface ID. The interface ID can be one of the following types:
  - Ethernet port
  - Port-channel.

Default Configuration

All interfaces.

Command Mode

Privileged EXEC mode

User Guidelines

This feature can only be used when working in RSTP or MSTP mode.

Example

This restarts the STP migration process on all interfaces.

```
switchxxxxxx# clear spanning-tree detected-protocols
```

52.18. spanning-tree mst priority

Use the `spanning-tree mst priority` Global Configuration mode command to configure the device priority for the specified spanning-tree instance. Use the no form of this command to restore the default configuration.

Syntax

- spanning-tree mst priority instance-id priority
- no spanning-tree mst instance-id priority

Parameters

- instance-id - Specifies the spanning-tree instance ID. (Range:1–15)
- priority - Specifies the device priority for the specified spanning-tree instance. This setting determines the likelihood that the switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch. (Range: 0–61440)

Default Configuration

The default priority is 32768.

Command Mode

Global Configuration mode

User Guidelines

The priority value must be a multiple of 4096.

The switch with the lowest priority is the root of the spanning tree.

Example

The following example configures the spanning tree priority of instance 1 to 4096.

```
switchxxxxxx(config)# spanning-tree mst 1 priority 4096
```

52.19. spanning-tree mst max-hops

Use the `spanning-tree mst max-hops` Global Configuration mode command to configure the number of hops in an MST region before the BDPU is discarded and the port information is aged out. Use the no form of this command to restore the default configuration.

Syntax

- spanning-tree mst max-hops hop-count
- no spanning-tree mst max-hops

Parameters

- max-hops hop-count - Specifies the number of hops in an MST region before the BDPU is discarded. (Range: 1–40)

Default Configuration

The default number of hops is 20.

Command Mode

Global Configuration mode

Example

The following example configures the maximum number of hops that a packet travels in an MST region before it is discarded to 10.

```
switchxxxxxx(config)# spanning-tree mst max-hops 10
```

52.20. spanning-tree mst port-priority

Use the `spanning-tree mst port-priority` Interface (Ethernet, Port Channel) Configuration mode command to configure the priority of a port. Use the no form of this command to restore the default configuration.

Syntax

- spanning-tree mst port-priority instance-id priority
- no spanning-tree mst instance-id port-priority

Parameters

- instance-id - Specifies the spanning tree instance ID. (Range: 1–15)
- priority - Specifies the port priority. (Range: 0–240 in multiples of 16)

Default Configuration

The default port priority is 128.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The priority value must be a multiple of 16.

Example

The following example configures the port priority of `te1/0/`1 to 144.

```
switchxxxxxx(config)# interface te1/0/1
```

```
switchxxxxxx(config-if)# spanning-tree mst 1 port-priority 144
```

52.21. spanning-tree mst cost

Use the `spanning-tree mst cost` Interface (Ethernet, Port Channel) Configuration mode command to configure the path cost for MST calculations. If a loop occurs, the spanning tree considers path cost when selecting an interface to put in the Forwarding state. Use the no form of this command to restore the default configuration.

Syntax

- spanning-tree mst cost instance-id cost
- no spanning-tree mst cost instance-id

Default Configuration

N/A

Parameters

- instance-id - Specifies the spanning-tree instance ID. (Range: 1–15)
- cost - Specifies the port path cost. (Range: 1–200000000)

Default Configuration

Default path cost is determined by the port speed and path cost method (long or short) as shown below:

Interface	Long	Short
Port-channel	20,000	4
TenGigabit Ethernet (10000 Mbps)		

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example configures the MSTP instance 1 path cost for port `te1/0/9` to 4.

```
switchxxxxxx(config)# interface te1/0/9
switchxxxxxx(config-if)# spanning-tree mst 1 cost 4
```

52.22. spanning-tree mst configuration

Use the `spanning-tree mst configuration` Global Configuration mode command to enable configuring an MST region by entering the MST mode.

Syntax

- spanning-tree mst configuration

Command Mode

Global Configuration mode

User Guidelines

For two or more switches to be in the same MST region, they must contain the same VLAN mapping, the same configuration revision number, and the same name.

Example

The following example configures an MST region.

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# instance 1 vlan 10-20
switchxxxxxx(config-mst)# name region1
switchxxxxxx(config-mst)# revision 1
```

52.23. instance (MST)

Use instance MST Configuration mode command to map VLANs to an MST instance. Use the no form of this command to restore the default mapping.

Syntax

- instance instance-id vlan vlan-range
- no instance instance-id vlan vlan-range

Parameters

- instance-id - MST instance (Range: 1–15)
- vlan-range - The specified range of VLANs is added to the existing ones. To specify a range, use a hyphen. To specify a series, use a comma. (Range: 1– 4094)

Default Configuration

All VLANs are mapped to the common and internal spanning tree (CIST) instance (instance 0).

Command Mode

MST Configuration mode

User Guidelines

All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST.

For two or more devices to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

Example

The following example maps VLANs 10-20 to MST instance 1.

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# instance 1 vlan 10-20
```

52.24. name (MST)

Use the `name` MST Configuration mode command to define the MST instance name. Use the no form of this command to restore the default setting.

Syntax

- name string
- no name

Parameters

- string - Specifies the MST instance name. (Length: 1–32 characters)

Default Configuration

The default name is the bridge MAC address.

Command Mode

MST Configuration mode

Example

The following example defines the instance name as Region1.

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# name region1
```

52.25. revision (MST)

Use the `revision` MST Configuration mode command to define the MST configuration revision number. Use the no form of this command to restore the default configuration.

Syntax

- revision value
- no revision

Parameters

- value - Specifies the MST configuration revision number. (Range: 0–65535)

Default Configuration

The default configuration revision number is 0.

Command Mode

MST Configuration mode

Example

The following example sets the configuration revision to 1.

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst) # revision 1
```

52.26. show (MST)

Use the `show` MST Configuration mode command to display the current or pending MST region configuration.

Syntax

- show {current | pending}

Parameters

- current - Displays the current MST region configuration.
- pending - Displays the pending MST region configuration.

Default Configuration

N/A

Command Mode

MST Configuration mode

Example

The following example displays a pending MST region configuration

```
switchxxxxxx(config-mst)# show pending
Gathering information ..........
Current MST configuration
Name: Region1
Revision: 1
Instance VLANs Mapped State
-------- ---------------------- ----
0 1-4094 Disabled
switchxxxxxx(config-mst)#
```

52.27. exit (MST)

Use the `exit` MST Configuration mode command to exit the MST region Configuration mode and apply all configuration changes.

Syntax

- exit

Parameters

N/A

Default Configuration

N/A

Command Mode

MST Configuration mode

Example

The following example exits the MST Configuration mode and saves changes.

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# exit
switchxxxxxx(config)#
```

52.28. abort (MST)

Use the `abort` MST Configuration mode command to exit the MST Configuration mode without applying the configuration changes.

Syntax

- abort

Parameters

N/A

Default Configuration

N/A

Command Mode

MST Configuration mode

Example

The following example exits the MST Configuration mode without saving changes.

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# abort
```

52.29. show spanning-tree

Use the `show spanning-tree` Privileged EXEC mode command to display the spanning-tree configuration.

Syntax

- show spanning-tree [interface-id] [instance instance-id] show spanning-tree [detail] [active | blockedports] [instance instance-id]
- show spanning-tree mst-configuration

Parameters

- instance instance-id - Specifies the spanning tree instance ID. (Range: 1–15).
- detail - Displays detailed information.
- active - Displays active ports only.
- blockedports - Displays blocked ports only.
- mst-configuration - Displays the MST configuration identifier.
- interface-id - Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

If no interface is specified, the default is all interfaces.

Command Mode

Privileged EXEC mode

User Guidelines

This command only works when MST is enabled.

Example

The following examples display spanning-tree information in various configurations

```
switchxxxxxx# show spanning-tree
Spanning tree enabled mode RSTP
Default port cost method: long
Loopback guard: Disabled
Root ID     Priority 32768
 Address 00:01:42:97:e0:00
 Cost 20000
 Port te1/0/1
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 36864
 Address 00:02:4b:29:7a:00
```

```
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Interfaces
Name State Prio. No Cost Sts Role PortFast Type
---- ----- -------- ---- --- ---- -------- ----
te1/0/1 Enabled 128.1 20000 FRW Root No P2p (RSTP)
te1/0/2 Enabled 128.2 20000 FRW Desg No Shared (STP)
te1/0/3 Disabled 128.3 20000 - - - -
te1/0/4 Enabled 128.4 20000 BLK Altn No Shared (STP)
te1/0/5 Enabled 128.5 20000 DIS - - -
switchxxxxxx# show spanning-tree
Spanning tree enabled mode RSTP
Default port cost method: long
Root ID Priority 36864
 Address 00:02:4b:29:7a:00
 This switch is the Root.
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Interfaces
Name State Prio. No Cost Sts Role PortFast Type
---- ----- -------- ---- --- ---- -------- ----
te1/0/1 Enabled 128.1 20000 FRW Desg - P2p (RSTP)
te1/0/2 Enabled 128.2 20000 FRW Desg No Shared (STP)
te1/0/3 Disabled 128.3 20000 - - No -
te1/0/4 Enabled 128.4 20000 FRW Desg - Shared (STP)
te1/0/5 Enabled 128.5 20000 DIS - No -
switchxxxxxx# show spanning-tree
Spanning tree disabled (BPDU filtering) mode RSTP
Default port cost method: long
Root ID Priority N/A
 Address N/A
 Path Cost N/A
 Root Port N/A
 Hello Time N/A Max Age N/A Forward Delay N/A
Bridge ID Priority 36864
 Address 00:02:4b:29:7a:00
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Interfaces
Name State Prio. No Cost Sts Role PortFast Type
---- ----- -------- ---- --- ---- -------- ----
te1/0/1 Enabled 128.1 20000 - - - -
te1/0/2 Enabled 128.2 20000 - - - -
te1/0/3 Disabled 128.3 20000 - - - -
te1/0/4 Enabled 128.4 20000 - - - -
te1/0/5 Enabled 128.5 20000 - - - -
switchxxxxxx# show spanning-tree active
Spanning tree enabled mode RSTP
Default port cost method: long
Root ID Priority 32768
 Address 00:01:42:97:e0:00
 Path Cost 20000
 Root Port te1/0/1
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 36864
 Address 00:02:4b:29:7a:00
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Interfaces
Name State Prio. No Cost Sts Role PortFast Type
```

```
---- ----- -------- ---- --- ---- -------- ----
te1/0/1 Enabled 128.1 20000 FRW Root - P2p (RSTP)
te1/0/2 Enabled 128.2 20000 FRW Desg No Shared (STP)
te1/0/4 Enabled 128.4 20000 BLK Altn No Shared (STP)
  No
switchxxxxxx# show spanning-tree blockedports
Spanning tree enabled mode
RSTP Default port cost method: long
Root ID Priority 32768
 Address 00:01:42:97:e0:00
 Path Cost 20000
 Root Port te1/0/1
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 36864
 Address 00:02:4b:29:7a:00
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Interfaces
Name State Prio. No Cost Sts Role PortFast Type
---- ----- -------- ---- --- ---- -------- ----
te1/0/4 Enabled 128.4 19 BLK Altn No Shared (STP)
switchxxxxxx# show spanning-tree detail
Spanning tree enabled mode RSTP
Default port cost method: long
Root ID Priority 32768
 Address 00:01:42:97:e0:00
 Path Cost 20000
 Root Port te1/0/1
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 36864
 Address 00:02:4b:29:7a:00
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Number of topology changes 2 last change occurred 2d18h ago
Times: hold 1, topology change 35, notification 2
 hello 2, max age 20, forward delay 15

Port 1 (te1/0/1) enabled
State: Forwarding Role: Root
Port id: 128.1 Port cost: 20000
Type: P2p (configured: auto) RSTP Port Fast: No (configured:no)
Designated bridge Priority: 32768 Address: 00:01:42:97:e0:00
Designated port id: 128.25 Designated path cost: 0
Guard root: Disabled BPDU guard: Disabled
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638
Port 2 (te1/0/2) enabled
State: Forwarding Role: Designated
Port id: 12 Port cost: 20000
Type: Shared (configured: auto) STP Port Fast: No (configured:no)
Designated bridge Priority: 32768 Address: 00:02:4b:29:7a:00
Designated port id: 12 Designated path cost: 20000
Guard root: Disabled BPDU guard: Disabled
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638
Port 3 (te1/0/3) disabled
State: N/A Role: N/A
Port id: 128.3 Port cost: 20000
```

```
Type: N/A (configured: auto) Port Fast: N/A (configured:no)
Designated bridge Priority: N/A Address: N/A
Designated port id: N/A Designated path cost: N/A
Guard root: Disabled BPDU guard: Disabled
Number of transitions to forwarding state: N/A
BPDU: sent N/A, received N/A
Port 4 (te1/0/4) enabled
State: Blocking Role: Alternate
Port id: 128.4 Port cost: 20000
Type: Shared (configured:auto) STP Port Fast: No (configured:no)
Designated bridge Priority: 28672 Address: 00:30:94:41:62:c8
Designated port id: 128.25 Designated path cost: 20000
Guard root: Disabled BPDU guard: Disabled
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638
Port 5 (te1/0/5) enabled
State: Disabled Role: N/A
Port id: 128.5 Port cost: 20000
Type: N/A (configured: auto) Port Fast: N/A (configured:no)
Designated bridge Priority: N/A Address: N/A
Designated port id: N/A Designated path cost: N/A
Guard root: Disabled BPDU guard: Disabled
Number of transitions to forwarding state: N/A
BPDU: sent N/A, received N/A
switchxxxxxx# show spanning-tree ethernet te1/0/1
Port 1 (te1/0/1) enabled
State: Forwarding Role: Root
Port id: 128.1 Port cost: 20000
Type: P2p (configured: auto) RSTP Port Fast: No (configured:no)
Designated bridge Priority: 32768 Address: 00:01:42:97:e0:00
Designated port id: 128.25 Designated path cost: 0
Guard root: Disabled BPDU guard: Disabled
Number of transitions to forwarding state: 1 BPDU: sent 2, received 120638
switchxxxxxx# show spanning-tree mst-configuration
Name: Region1
Revision: 1
Instance Vlans mapped State
-------- ------------ -----
1 1-9, 21-4094 Enabled
2 10-20 Enabled
switchxxxxxx# show spanning-tree
Spanning tree enabled mode MSTP
Default port cost method: long
###### MST 0 Vlans Mapped: 1-9
CST Root ID Priority 32768
 Address 00:01:42:97:e0:00
 Path Cost 20000
 Root Port te1/0/1
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

IST Master ID Priority 32768
 Address 00:02:4b:29:7a:00
 This switch is the IST master.
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Max hops 20
```

```
Interfaces
Name State Prio. No Cost Sts Role PortFast Type
---- ----- -------- ---- --- ---- -------- ----
te1/0/1 Enabled 128.1 20000 FRW Root No P2p Bound (RSTP)
te1/0/2 Enabled 128.2 20000 FRW Desg No Shared Bound (RSTP)
te1/0/3 Disabled 128.3 20000 FRW Desg No p2p
te1/0/4 Enabled 128.4 20000 FRW Desg No p2p

###### MST 1 Vlans Mapped: 10-20
Root ID Priority 24576
 Address 00:02:4b:29:89:76
 Path Cost 20000
 Root Port te1/0/4
 Rem hops 19

Bridge ID Priority 32768
 Address 00:02:4b:29:7a:00
Interfaces
Name State Prio. No Cost Sts Role PortFast Type
---- ----- -------- ---- --- ---- -------- ----
te1/0/1 Enabled 128.1 20000 FRW Boun No P2p Bound (RSTP)
te1/0/2 Enabled 128.2 20000 FRW Boun No Shared Bound (RSTP)
te1/0/3 Disabled 128.3 20000 BLK Altn No p2p
te1/0/4 Enabled 128.4 20000 FRW Boun No p2p

switchxxxxxx# show spanning-tree detail
Spanning tree enabled mode MSTP
Default port cost method: long
###### MST 0 Vlans Mapped: 1-9
CST Root ID Priority 32768
 Address 00:01:42:97:e0:00
 Path Cost 20000
 Root Port te1/0/1
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

IST Master ID Priority 32768
 Address 00:02:4b:29:7a:00
 This switch is the IST master.
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Max hops 20
 Number of topology changes 2 last change occurred 2d18h ago
 Times: hold 1, topology change 35, notification 2
 hello 2, max age 20, forward delay 15

Port 1 (te1/0/1) enabled
State: Forwarding Role: Root
Port id: 128.1 Port cost: 20000
Type: P2p (configured: auto) Boundary RSTP Port Fast: No (configured:no)
Designated bridge Priority: 32768 Address: 00:01:42:97:e0:00
Designated port id: 128.25 Designated path cost: 0
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

Port 2 (te1/0/2) enabled
State: Forwarding Role: Designated
Port id: 128.2 Port cost: 20000
```

```
Type: Shared (configured: auto) Boundary STP Port Fast: No (configured:no)
Designated bridge Priority: 32768 Address: 00:02:4b:29:7a:00
Designated port id: 128.2 Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Port 3 (te1/0/3) enabled
State: Forwarding Role: Designated
Port id: 128.3 Port cost: 20000
Type: Shared (configured: auto) Internal Port Fast: No (configured:no)
Designated bridge Priority: 32768 Address: 00:02:4b:29:7a:00
Designated port id: 128.3 Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Port 4 (te1/0/4) enabled
State: Forwarding Role: Designated
Port id: 128.4 Port cost: 20000
Type: Shared (configured: auto) Internal Port Fast: No (configured:no)
Designated bridge Priority: 32768 Address: 00:02:4b:29:7a:00
Designated port id: 128.2 Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

###### MST 1 Vlans Mapped: 10-20
Root ID Priority 24576
 Address 00:02:4b:29:89:76
 Path Cost 20000
 Root Port te1/0/4
 Rem hops 19

Bridge ID Priority 32768
 Address 00:02:4b:29:7a:00
 Number of topology changes 2 last change occurred 1d9h ago
 Times: hold 1, topology change 2, notification 2
 hello 2, max age 20, forward delay 15

Port 1 (te1/0/1) enabled
State: Forwarding Role: Boundary
Port id: 128.1 Port cost: 20000
Type: P2p (configured: auto) Boundary RSTP Port Fast: No (configured:no)
Designated bridge Priority: 32768 Address: 00:02:4b:29:7a:00
Designated port id: 128.1 Designated path cost: 0
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

Port 2 (te1/0/2) enabled
State: Forwarding Role: Designated
Port id: 128.2 Port cost: 20000
Type: Shared (configured: auto) Boundary STP Port Fast: No (configured:no)
Designated bridge Priority: 32768 Address: 00:02:4b:29:7a:00
Designated port id: 128.2 Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Port 3 (te1/0/3) enabled
```

```
State: Blocking Role: Designated
Port id: 128.3 Port cost: 20000
Type: Shared (configured: auto) Internal Port Fast: No (configured:no)
Designated bridge Priority: 32768 Address: 00:02:4b:29:1a:19
Designated port id: 128.3 Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Port 4 (te1/0/4) enabled
State: Forwarding Role: Designated
Port id: 128.4 Port cost: 20000
Type: Shared (configured: auto) Internal Port Fast: No (configured:no)
Designated bridge Priority: 32768 Address: 00:02:4b:29:7a:00
Designated port id: 128.2 Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638
switchxxxxxx# show spanning-tree
Spanning tree enabled mode MSTP
Default port cost method: long
###### MST 0 Vlans Mapped: 1-9
CST Root ID Priority 32768
 Address 00:01:42:97:e0:00
 Path Cost 20000
 Root Port te1/0/1
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

IST Master ID Priority 32768
 Address 00:02:4b:29:7a:00
 Path Cost 10000
 Rem hops

Bridge ID Priority 32768
 Address 00:02:4b:29:7a:00
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Max hops 20
switchxxxxxx# show spanning-tree Spanning tree enabled mode MSTP
Default port cost method: long
###### MST 0 Vlans Mapped: 1-9
CST Root ID Priority 32768
 Address 00:01:42:97:e0:00
 Path Cost 20000
 Root Port te1/0/1
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Max hops 20
```

52.30. show spanning-tree bpdu

Use the `show spanning-tree bpdu` User EXEC mode command to display the BPDU handling when spanning-tree is disabled.

Syntax

- show spanning-tree bpdu [interface-id | detailed]

Parameters

- interface-id - Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

- detailed - Displays information for non-present ports in addition to present ports.

Default Configuration

Show information for all interfaces. If detailed is not used, only present ports are displayed.

Command Mode

User EXEC mode

Example

The following examples display spanning-tree BPDU information:

```
switchxxxxxx# show spanning-tree bpdu
The following is the output if the global BPDU handling command is not
supported.

Interface Admin Mode Oper Mode
--------- ---------- ---------
te1/0/1 Filtering Filtering
te1/0/2 Filtering Filtering
te1/0/3 Filtering Guard

The following is the output if both the global BPDU handling command and the
per-interface BPDU handling command are supported. Global: Flooding

Interface Admin Mode Oper Mode
--------- ---------- ---------
te1/0/1 Global Flooding
te1/0/2 Global STP
te1/0/3 Flooding STP
```

52.31. spanning-tree loopback-guard

Use the `spanning-tree loopback-guard` Global Configuration command to shut down an interface if it receives a loopback BPDU. Use the no form of this command to return the default setting.

Syntax

- spanning-tree loopback-guard
- no spanning-tree loopback-guard

Parameters

N/A

Default Configuration

N/A

Command Mode

Global

User Guidelines

This enables shutting down all interfaces if a loopback BPDU is received on it.

Example

```
switchxxxxxx(config)# spanning-tree loopback-guard
```

53. RRP Configuration

Note:
Please observe the notes regarding the use of RRP with different firmware versions on page 36.

Note:
The switch supports either the standard Redundant Ring Protocol (RRP) or the MICROSENS Redundant Ring Protocol (MRRP), depending on the firmware version of the switch. Both protocols are realised via the command `rrp` and cannot be used simultaneously. Please direct any questions concerning the ring protocol implementation to the device manufacturer.

Note:
Ports that belong to the ring should be properly configured to ensure correct RRP operation.

Primary operations for it are adding/removing VLAN to/from port and configuring tagged/untagged mode for packets that belong to added VLANs.

Both control VLAN and a set of data VLANs must be explicitly enabled on the ring ports.

For more information on the respective switchport commands please refer to the sections “59.11 switchport mode” on page 699 and “59.15 switchport general allowed vlan” on page 703.

53.1. Information on Ring Health Polling

The master node sends a health-check frame on the control VLAN at a user-configurable interval. If the ring is complete the health-check frame will be received on its secondary port, where the master node will reset its fail-period timer and continue normal operation.

If the master node does not receive the health-check frame before the fail-period timer expires the master node moves from the normal state to the “failed” state and unblocks its secondary port. The master node also flushes its bridging table and sends a control frame to all other nodes instructing them to also flush their bridging tables. Immediately after flushing its bridge table each node starts learning the new topology. This ring polling mechanism provides a backup in the event that the “link-down” alert frame should get lost for some unforeseen reason.

Example

The following command sets the fail timer to 4 seconds:

```
rrp fail-timer 4
```

In case the health timer is set to 1 second (default value, the most frequent one) it means that due to the fail-timer setting we are waiting for 4 seconds until treating the ring as broken.

The ring will react longer but there are less chances of incorrect detection of a broken link (if at least one health packet out of four is delivered then the ring is treated as functional).

53.2. Information on General RRP Timer Configuration

Health timer should be set to 1 second (the smallest possible value).

The more seconds you assign to the fail timer the more time it may take for the ring to recover in case of a broken link but with less chances to have “false positive” detection of a broken ring (or loop in the ring).

Best way to find a feasible value for the fail timer in the existing network infrastructure is a try-and-test approach.

53.3. RRP

Use the command `rrp` in Global Configuration mode to globally enable an RRP (Ring Redundancy Protocol) functionality.

Use the `no` form of this command to disable the RRP functionality globally.

Syntax

- rrp
- no rrp

Default Configuration

RRP is disabled.

Command Mode

Global Configuration mode.

User Guidelines

This command enables RRP functionality on current device. RRP is disabled by default.

Example

The following example enables RRP functionality globally:

```
console(config)# rrp
```

53.4. RRP mode

Use the command `rrp mode` in Global Configuration mode to select RRP mode.

Use the `no` form of this command to restore the default configuration.

Syntax

- rrp mode {srrp|mrrp}
- no rrp mode

Parameters

- srrp - sets RRP mode to Standard RRP (SRRP)
- mrrp - sets RRP mode to MICROSENS RRP (MRRP)

Default Configuration

The default RRP mode is SRRP.

Command Mode

Global Configuration mode

User Guidelines

This command configures the RRP mode on the current device.

Note:
Changing the RRP mode is not possible while RRP is enabled. RRP functionality must be disabled globally (use command `no rrp`) first in order to change RRP mode. After changing the RRP mode, enable RRP globally (use command `rrp`).

Example

The following example enables MRRP mode:

```
console(config)# rrp mode mrrp
```

53.5. RRP fail-timer (SRRP)

In SRRP mode, use the command `rrp fail-timer` in Global configuration mode to configure the fail timer interval.

Use the no form of this command to restore default configuration.

Syntax

- rrp fail-timer seconds
- no rrp fail-timer

Parameters

- seconds - Specifies the SRRP Fail time in seconds. (Range: 2–5)

Default Configuration

The default fail time for SRRP is 2 seconds.

Command Mode

Global Configuration mode.

Example

The following example configures the SRRP fail time to 5 seconds.

```
console(config)# rrp fail-timer 5
```

53.6. RRP health-timer (SRRP)

In SRRP mode, use the command `rrp health-timer` in Global configuration mode to configure the health timer interval.

Use the `no` form of this command to restore default configuration.

Syntax

- rrp health-timer seconds
- no rrp health-timer

Parameters

- seconds - Specifies the SRRP Hello time in seconds. (Range: 1–2)

Default Configuration

The default health timer interval for SRRP is 1 seconds.

Command Mode

Global Configuration mode.

Example

The following example configures the SRRP health timer interval to 2 seconds.

```
console(config)# rrp health-timer 2
```

53.7. RRP domain

Use the command `rrp domain` in Global Configuration mode to enter the RRP Domain Configuration mode.

Use `no` form of this command to delete a domain.

Syntax

- rrp domain domain-id
- no rrp domain domain-id

Parameters

- domain-id - Specifies the domain number. (Range: 0–15)

Command Mode

Global Configuration mode.

User Guidelines

You can use the command `no rrp domain` to delete domain with given Id only if it does not contain enabled rrp rings.

Example

The following example enters to the domain context number 4.

```
console(config)# rrp domain 4
console(config-rrp-domain)#
```

The following example attempts to delete domain number 5.

```
console(config)# no rrp domain 5
```

53.8. Control Vlan

Use the command `control vlan` in RRP Domain in Configuration mode to configure the control VLAN for current domain.

Use the `no` form to this command to delete control VLAN settings for current domain.

Syntax

- control-vlan vlan-id
- no control-vlan

Parameters

- domain-id - RRP primary control VLAN id range. (Range: 1–4093)

Command Mode

RRP Domain Configuration mode.

User Guidelines

The command control-vlan is used for setting a control VLAN number for current domain.

Change the control VLAN by first deleting it and then configure it anew.

Note:
The control VLAN must be specified in domain for its ring to be operational. Additionally, control VLAN must be created in system VLAN database and enabled on ring ports. Ring will

remain in IDLE state even after global and local admin enable unless aforementioned requirements are satisfied.

Example

The following example set the control VLAN to 77.

```
console(config-rrp-domain)# control-vlan 77
```

53.9. Ring

Use the command `ring` in the RRP Domain Configuration mode to enter the RRP Ring Configuration mode.

Use `no` form of this command to delete a ring.

Syntax

- rrp ring
- no rrp ring

Command Mode

RRP Domain Configuration mode

User Guidelines

The command `rrp ring` is used to enter the ring context.

Example

The following example enters to the ring context number.

```
console(config-rrp-domain)# rrp ring
console(config-rrp-domain-ring)#
```

53.10. Role

Use thecommand `role` RRP in Ring Configuration mode to configure a role for the current ring.

Syntax

- role {master|transit}

Command Mode

RRP Ring Configuration mode.

User Guidelines

The command `rrp role` is used for setting a role in RRP. A role can be declared as master or transit.

Example

The following example sets the role for current ring as transit in sub ring.

```
console(config-rrp-domain-ring)# role transit
```

53.11. Primary port

Use the command `primary port` in RRP Ring Configuration mode to configure a primary port for the current ring.

Syntax

- primary-port primary-port-id

Parameters

- primary-port-id - Specifies a primary-port ID. The interface ID can be Ethernet port.

Command Mode

RRP Ring Configuration mode.

User Guidelines

The primary port command is used for setting a primary port to current ring. It means primary port for primary ring or common port for sub ring.

Example

The following example set the primary port as gigabitethernet 1/0/4.

```
console(config-rrp-domain)# primary-port gigabitethernet 1/0/4
```

53.12. Secondary port

Use the command `secondary port` in RRP Ring Configuration mode to configure a secondary port for the current ring.

Syntax

- secondary-port secondary-port-id

Parameters

- secondary-port-id - Specifies a secondary-port ID. The interface ID can be Ethernet port.

Command Mode

RRP Ring Configuration mode.

User Guidelines

The secondary port command is used for setting a secondary port to current ring. It means secondary port for primary ring or edge port for sub ring.

Example

The following example set the secondary port as gigabitethernet 1/0/4.

```
console(config-rrp-domain-ring)# secondary-port gigabitethernet 1/0/4
```

53.13. Guard port (SRRP)

In SRRP mode, use the command `guard port` in RRP Ring Configuration mode to configure a secondary port for the current ring.

Syntax

- guard-port {disable|primary|secondary|both}

Parameters

- disable — Specifies that no port in ring serves as guard port.
- primary — Specifies only primary ring port as a guard port.

- secondary — Specifies only secondary ring port as a guard port.
- both — Specifies both primary and secondary ring ports as guard ports..

Command Mode

RRP Ring Configuration mode.

User Guidelines

The guard port command is used for setting a secondary port to current ring. It means secondary port for primary ring or edge port for sub ring.

Example

The following example set the secondary port as gigabitethernet 1/0/4.

```
console(config-rrp-domain-ring)# secondary-port gigabitethernet 1/0/4
```

53.14. Number (MRRP)

In MRRP mode, use the command `number` in RRP Ring Configuration mode to configure ring number for the current ring.

Syntax

- number number_id

Parameters

- number_id - Specifies ring number. (Range: 0-255).

Default Configuration

The default ring number is 0.

Command Mode

RRP Ring Configuration mode.

User Guidelines

The command `number` is used for setting ring number to current ring in MRRP mode. Ring number must be identical for each member of a ring.

Example

The following example sets ring number to 1.

```
console(config-rrp-domain-ring)# number 1
```

53.15. Ring enable

Use thecommand `ring enable` in RRP Domain Configuration mode to configure RRP admin state of the ring in a single domain.

Syntax

- set ring {enable|disable}

Command Mode

RRP Domain Configuration mode.

User Guidelines

This command manages ring admin enable/disable state.

Example

The following example enables ring.

```
console(config)# set ring enable
```

53.16. Show rrp

Use the command `show rrp` in EXEC mode to display information about the rrp configuration.

Syntax

- show rrp [domain domain-id]

Parameters

- domain-id - Specifies a domain ID to be shown.

Command Mode

EXEC mode.

User Guidelines

This command displays information about the rrp configuration. When running the command without parameters it displays all RRP configuration info.

Example

The following example shows all RRP configuration info.

```
console# show rrp

RRP state: Enable
RRP mode: Standard RRP (SRRP)
Time value: health 1s, failed 2s
domain info: domain-id 0, control-vlan 4000
  RRP Node Type       : transit
  Admin Status        : Enable
  Status              : Active
  Ring State          : linkDown
  Primary Port        : gi1/0/1 down
  Primary Port Role   : unknown
  Secondary Port      : gi1/0/2 down
  Secondary Port Role : unknown
  Ring Guard Port     : disable
Total 1 ring(s).
Total 1 domain(s), total 1 ring(s).
```

The following example shows all RRP configuration info in MRRP mode:

```
console# show rrp

RRP state: Enable
RRP mode: MICROSENS RRP (MRRP)
Domain 0, Control Vlan 4000
  RRP Node Type       : transit
  RRP Number          : 1
  Admin Status        : Enable
  Status              : Idle
```

```
  Primary Port         : gi1 down
  Secondary Port       : gi2 down
  Ring Interrupt       : false
  Global Alarm         : false
  Error Detected       : false
  Number of Backups    : 0
  Current Backup Time  : 00:00:00
  Total Backup Time    : 00:00:00
  Last Backup Time     : 00:00:00
Total 1 ring(s).
Total 1 domain(s), total 1 ring(s).
```

53.17. Port Configuration

Ports that belong to the ring should also be properly configured to ensure correct RRP operation.

Primary operations for it are adding/removing VLAN to/from port and configuring tagged/untagged mode for packets that belong to added VLANs.

Both control VLAN and a set of data VLANs must be explicitly enabled on the ring ports.

The following commands are necessary for such configuration:

- **switchport mode:** see section 59.11 on page 699.
- **switchport general allowed vlan:** see section 59.15 on page 703.

53.18. Configuration Examples

53.18.1. Single Master Ring in SRRP Mode

The following example configures a single master ring in SRRP mode with control VLAN 4000 and data VLAN 1.

```
rp
rrp domain 0
 control-vlan 4000
 ring
  role master
  primary-port gigabitethernet1/0/1
  secondary-port gigabitethernet1/0/2
  guard-port disable
 exit
 set ring enable
exit

vlan database
 vlan 4000
exit

interface gigabitethernet1/0/1
 switchport mode general
 switchport general allowed vlan add 4000 tagged
 switchport general allowed vlan add 1 untagged
exit

interface gigabitethernet1/0/2
 switchport mode general
 switchport general allowed vlan add 4000 tagged
 switchport general allowed vlan add 1 untagged
exit
```

53.18.2. Multiple Rings with Ring Guard in SRRP Mode

The following example configures two transit rings with control VLANs 4000, 4001 and data VLAN 1. The guard port is enabled on the primary port of the first ring.

```
rrp
rrp domain 0
 control-vlan 4000
 ring
  role transit
  primary-port fastethernet1/0/1
  secondary-port fastethernet1/0/2
  guard-port primary
 exit
 set ring enable
 exit
rrp domain 1
 control-vlan 4001
 ring
  role transit
  primary-port fastethernet1/0/1
  secondary-port fastethernet1/0/3
  guard-port disable
 exit
 set ring enable
exit

vlan database
 vlan 4000-4001
exit

interface fastethernet1/0/1
 switchport mode general
 switchport general allowed vlan add 4000-4001 tagged
 switchport general allowed vlan add 1 untagged
exit

interface fastethernet1/0/2
 switchport mode general
 switchport general allowed vlan add 4000 tagged
 switchport general allowed vlan add 1 untagged
exit

interface fastethernet1/0/3
 switchport mode general
 switchport general allowed vlan add 4001 tagged
 switchport general allowed vlan add 1 untagged
exit
```

53.19. Master Ring in MRRP Mode

The following example configures a master ring in MRRP mode with control VLAN 4000 and data VLAN 1.

```
rrp
rrp mode mrrp
rrp domain 0
```

```
 control-vlan 4000
 ring
  role master
  primary-port gigabitethernet1
  secondary-port gigabitethernet2
  number 1
 exit
 set ring enable
exit

vlan database
 vlan 4000
exit

interface gigabitethernet1
 switchport mode general
 switchport general allowed vlan add 4000 tagged
 switchport general allowed vlan add 1 untagged
exit

interface gigabitethernet2
 switchport mode general
 switchport general allowed vlan add 4000 tagged
 switchport general allowed vlan add 1 untagged
exit
```

54. SSH Client Commands

54.1. ip ssh-client authentication

To define the SSH client authentication method used by the local SSH clients to be authenticated by remote SSH servers, use the `ip ssh-client authentication` command in Global Configuration mode.

To return to default, use the no format of the command.

Syntax

- ip ssh-client authentication {password | public-key {rsa | dsa}}
- no ip ssh-client authentication

Parameters

- password - Username and password are used for authentication.
- public-key rsa - Username and RSA public key are used for authentication.
- public-key dsa - Username and DSA public key are used for authentication.

Default Configuration

Username and password are used for authentication by the local SSH clients.

Command Mode

Global Configuration mode

User Guidelines

A user can use the `ip ssh-client key` command to generate/configure RSA/DSA keys if SSH authentication is by public key. Otherwise, the default keys generated by the switch are used.

Example

The following example specifies that, username and public key are used for authentication:

```
switchxxxxxx(config)# ip ssh-client authentication public-key rsa
```

54.2. ip ssh-client change server password

To change a password of an SSH client on a remote SSH server, use the `ip ssh-client change server password` command in Global Configuration mode.

Syntax

- ip ssh-client change server password server {host | ip-address | ipv6-address} username username old-password old-password new-password new-password

Parameters

- host - DNS name of a remote SSH server.
- ip-address - Specifies the IP address of a remote SSH server. The IP address can be an IPv4, IPv6 or IPv6 address. See IPv6 Address Conventions.
- username - Username of the local SSH clients (1 - 70 characters).
- old-password - Old password of the local SSH client (1 - 70 characters).
- new-password - New password for the local SSH client (1 - 70 characters). The password cannot include the characters "@" and ":".

Default Configuration

None

Command Mode

Global Configuration mode

User Guidelines

Use the command to change a password on a remote SSH server. Use the ip ssh-client password command to change the SSH client password of the switch’s SSH client so that it matches the new password set on the remote SSH server.

Example

The following example changes a password of the local SSH clients:

```
switchxxxxxx(config)# ip ssh-client change server password server 10.7.50.155
username john old-password &&&@@@aaff new-password &&&@@@aaee
```

54.3. ip ssh-client key

To create a key pair for SSH client authentication by public key (either by generating a key or by importing a key), use the `ip ssh-client key` command in Global Configuration mode. To remove a key, use the no form of the command.

Syntax

- ip ssh-client key {dsa | rsa} {generate | key-pair privkey pubkey}
- no ip ssh-client key [dsa | rsa]

Parameters

- dsa - DSA key type.
- rsa - RSA key type.
- key-pair - Key that is imported to the device.
- privkey - Plaintext private key.
- pubkey - The plaintext pubic key.

Default Configuration

The application creates a key automatically; this is the default key.

Command Mode

Global Configuration mode

User Guidelines

When using the keyword generate, a private key and a public key of the given type (RSA/DSA) are generated for the SSH client. Downloading a configuration file with a Key Generating command is not allowed, and such download will fail.

When using the keyword key-pair, the user can import a key-pair created by another device. In this case, the keys must follow the format specified by RFC 4716.

If the specified key already exists, a warning will be issued before replacing the existing key with a new key.

Use the no ip ssh-client key command to remove a key pair. Use this command without specifying a key-type to remove both key pairs.

Table 2 describes the expected behavior of keys, default and users within the various operations.

Table 2: Keys, Defaults and Users

From/To	Show	Show (detailed)	Copy/Upload of Running Config	Copy/Upload of Startup Config	Download text-based CLI (TFTP/Backup)
Startup Config	Only user-defined	N/A	All keys (default and user)	N/A	All keys (default and user)
Running Config	Keys are not displayed.	All keys (default and user)	N/A	Only user defined.	Same as user configuration
Text-based CLI (TFTP/Backup)	As it was copied.	N/A	All keys (default and user)	Only user defined.	As a text file.

If no keys are included in text-based configuration file, the device generates it's own keys during initialization. If the Running Configuration contains default keys (not user-defined), the same default keys remain.

Examples

Example 1 - In the following example, a key pair of the RSA type is created:

```
switchxxxxxx(config)# ip ssh-client key rsa generate The SSH service is
generating a private RSA key.
This may take a few minutes, depending on the key size.
```

Example 2 - In the following example, both public and private keys of the RSA type are imported (private key as plaintext):

```
switchxxxxxx(config)# ip ssh-client key rsa key-pair
Please paste the input now, add a period (.) on a separate line after the input
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDH6CU/2KYRl8rYrK5+TIvwS4zvhBmiC4I31m9cR/1iRTFViMRuJ++TEr
p9ssqWyI1Ti9d0jzmG0N3jHzp2je5/DUTHZXvYaUzchBDnsPTJo8dyiBl4YBqYHQgCjUhk
tXqvloy+1uxRJTAaLVXCBAmuIU/kMLoEox8/zwjB/jsF9wIBIwKBgC2xZ5mQmvy0+yo2GU
FwlQO5f0yweuM11J8McTmqDgfVTRrdbroXwbs3exVqsfaUPY9wa8Le6JPX+DPp4XovEfC/
iglZBSC8SeDmI2U7D6HrkAyD9HHf/r32jukB+5Z7BlHPz2Xczs2clOOwrnToy+YTzjLUxy
WS7V/IxbBllipLAkEA/QluVSCfFmdMlZxaEfJVzqPO1cF8guovsWLteBf/gqHuvbHuNy0t
OWEpObKZs1m/mtCWppkgcqgrB0oJaYbUFQJBAMo/cCrkyhsiV/+ZsryeD26NbPEKiak16V
Tz2ayDstidGuuvcvm2YF7DjM6n6NYz3+/ZLyc5n82okbld1NhDONsCQQCmSAas+C4HaHQn
zSU+/lWlDI88As4qJN2DMmGJbtsbVHhQxWIHAG4tBVWa8bV12+RPyuan/jnk8irniGyVza
FPAkEAiq8oV+1XYxA8V39V/a42d7FvRjMckUmKDl4Rmt32+u9i6sFzaWcdgs87+2vS3AZQ
afQDE5U6YSMiGLVewC4YWwJBAOFZmhO+dIlxT8Irzf2cUZGggopfnX6Y+L+Yl09MuZHbwH
tXaBGj6ayMYvXnloONecnApBjGEm37YVwKjO2DV2w=
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY----
MIGHAoGBAMfoJT/YphGXytisrn5Mi/BLjO+EGaILgjfWb1xH/WJFMVWIxG4n75MSun2yyp
```

```
bIjVOL13SPOYbQ3eMfOnaN7n8NRMdle9hpTNyEEOew9Mmjx3KIGXhgGpgdCAKNSGS1eq+W
jL7W7FElMBotVcIECa4hT+QwugSjHz/PCMH+OwX3AgEj
-----END RSA PUBLIC KEY----.
```

Example 3 - In the following example, both public and private keys of the DSA type are imported (private key as encrypted):

```
switchxxxxxx(config)# encrypted ip ssh-client key rsa key-pair
(Need to encrypted SSH client RSA key pair, for example:)
-----BEGIN RSA ENCRYPTED PRIVATE KEY----
gxeOjs6OzGRtL4qstmQg1B/4gexQblfa56RdjgHAMejvUT02elYmNi+m4aTu6mlyXPHmYP
lXlXny7jZkHRvgg8EzcppEB0O3yQzq3kNi756cMg4Oqbkm7TUOtdqYFEz/h8rJJ0QvUFfh
BsEQ3e16E/OPitWgK43WTzedsuyFeOoMXR9BCuxPUJc2UeqQVM2IJt5OM0FbVt0S6oqXhG
sEEdoTlhlDwHWg97FcV7x+bEnPfzFGrmbrUxcxOxlkFsuCNo3/94PHK8zEXyWtrx2KoCDQ
qFRuM8uecpjmDh6MO2GURUVstctohEWEIVCIOr5SBCbciaxv5oS0jIzXMrJA==
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBALLOeh3css8tBL8ujFt3trcX0XJyJLlxxt4sGp8Q3ExlSRN25+Mcac6togpIEg
tIzk6t1IEJscuAih9Brwh1ovgMLRaMe25j5YjO4xG6Fp42nhHiRcie+YTS1o309EdZkiXa
QeJtLdnYL/r3uTIRVGbXI5nxwtfWpwEgxxDwfqzHAgEj
-----END RSA PUBLIC KEY-----
```

Example 4 - In the following example, a DSA key pair is removed:

```
switchxxxxxx(config)# no ip ssh-client key dsa
```

Example 5 - In the following example, all key pairs (RSA and DSA types) are removed.

```
switchxxxxxx(config)# no ip ssh-client key
```

54.4. ip ssh-client password

To configure the password for SSH client authentication by password, use the `ip ssh-client password` command in Global Configuration mode. To return to default, use the no form of the command.

Syntax

- ip ssh-client password string
- no ip ssh-client password

Parameters

- string - Password for the SSH clients (1 - 70 characters). The password cannot include the characters "@" and ":".

Default Configuration

The default password is anonymous.

Command Mode

Global Configuration mode

User Guidelines

If authentication is configured to use a password (using the command ip ssh-client authentication), use the ip ssh-client password command to define the password.

Use the command ip ssh-client change server password to change the password on the remote SSH server so that it will match the new password of the SSH client.

Example

The following example specifies a plaintext password for the local SSH clients:

```
switchxxxxxx(config)# ip ssh-client password &&&111aaff
```

54.5. ip ssh-client server authentication

To enable remote SSH server authentication by the SSH client, use the `ip ssh-client server authentication` command in Global Configuration mode.

To disable remote SSH server authentication, use the no form of the command.

Syntax

- ip ssh-client server authentication
- no ip ssh-client server authentication

Parameters

This command has no arguments or keywords.

Default Configuration

SSH server authentication is disabled

Command Mode

Global Configuration mode

User Guidelines

When remote SSH server authentication is disabled, any remote SSH server is accepted (even if there is no entry for the remote SSH server in the SSH Trusted Remote Server table).

When remote SSH server authentication is enabled, only trusted SSH servers are accepted. Use the ip ssh-client server fingerprint command to configure trusted SSH servers.

Example

The following example enables SSH server authentication:

```
switchxxxxxx(config)# ip ssh-client server authentication
```

54.6. ip ssh-client server fingerprint

To add a trusted server to the Trusted Remote SSH Server Table, use the `ip ssh-client server fingerprint` command in Global configuration mode. To remove an entry or all entries from the Trusted Remote SSH Server Table, use the no form of the command.

Syntax

- ip ssh-client server fingerprint {host | ip-address} fingerprint
- no ip ssh-client server fingerprint [host | ip-address]

Parameters

- host - DNS name of an SSH server.
- ip-address - Specifies the address of an SSH server. The IP address can be an IPv4, IPv6 or IPv6 address. See IPv6 Address Conventions.
- fingerprint - FIngerprint of the SSH server public key (32 Hex characters).

Default Configuration

The Trusted Remote SSH Server table is empty.

Command Mode

Global Configuration mode

User Guidelines

Fingerprints are created by applying a cryptographic hash function to a public key. Fingerprints are shorter than the keys they refer to, making it simpler to use (easier to manually input than the original key). Whenever the switch is required to authenticate an SSH server's public key, it calculates the received key's fingerprint and compares it to the previously-configured fingerprint.

The fingerprint can be obtained from the SSH server (the fingerprint is calculated when the public key is generated on the SSH server).

The no ip ssh-client server fingerprint command removes all entries from the Trusted Remote SSH Server table.

Example

In the following example, a trusted server is added to the Trusted Servers table (with and without a separator ":"):

```
switchxxxxxx(config)# ip ssh-client server fingerprint 1.1.1.1
DC789788DC88A988127897BCBB789788
switchxxxxxx(config)# ip ssh-client server fingerprint 1.1.1.1
DC:78:97:88:DC:88:A9:88:12:78:97:BC:BB:78:97:88
```

54.7. ip ssh-client source-interface

To specify the source interface which IPv4 address will be used as the Source IPv4 address for communication with IPv4 SSH servers, use the `ip ssh-client source-interface` Global Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- ip ssh-client source-interface interface-id
- no ip ssh-client source-interface

Parameters

- interface-id - Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface then the interface IP address belonging to next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface then the minimal IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 SSH servers.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# ip ssh-client source-interface vlan 100
```

54.8. ipv6 ssh-client source-interface

To specify the source interface whose IPv6 address will be used as the Source IPv6 address for communication with IPv6 SSH servers, use the `ipv6 ssh-client source-interface` Global Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- ipv6 ssh-client source-interface interface-id
- no ipv6 ssh-client source-interface

Parameters

- interface-id - (Optional) Specifies the source interface.

Default Configuration

The IPv6 source address is the IPv6 address defined of the outgoing interface and selected in accordance with RFC6724.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface then the IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

If the source interface is not the outgoing interface then the minimal IPv4 address defined on the source interface and with the scope of the destination IPv6 address is applied.

If there is no available IPv6 source address, a SYSLOG message is issued when attempting to communicate with an IPv6 SSH servers.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# ipv6 ssh-client source-interface vlan 100
```

54.9. ip ssh-client username

To configure the SSH client username of the switch, use the `ip ssh-client username` command in Global Configuration mode.

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

Syntax

- ip ssh-client username string

- no ip ssh-client username

Parameters

string - Username of the SSH client.The length is 1 - 70 characters. The username cannot include the characters "@" and ":".

Default Configuration

The default username is anonymous

Command Mode

Global Configuration mode

User Guidelines

The configured username is used when SSH client authentication is done both by password or by key.

Example

The following example specifies a username of the SSH client:

```
switchxxxxxx(config)# ip ssh-client username jeff
```

54.10. show ip ssh-client

To display the SSH client credentials, both default and user-defined keys, use the `show ip ssh-client` command in Privilege EXEC mode.

Syntax

- show ip ssh-client show ip ssh-client {mypubkey | key} {dsa | rsa}

Parameters

- dsa - Specifies displaying the DSA key type.
- rsa - Specifies displaying the RSA key type.
- mypubkey - Specifies that only the public key is selected to be displayed.

Command Mode

Privileged EXEC mode

User Guidelines

Use the command with a specific key-type to display the SSH client key; You can either specify display of public key or private key, or with no parameter to display both private and public keys. The keys are displayed in the format specified by RFC 4716.

Examples

Example 1. The following example displays the authentication method and the RSA public key:

```
switchxxxxxx# show ip ssh-client mypubkey rsa
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
Authentication method: DSA key
Username: john
Key Source: User Defined
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
```

```
AAAAB3NzaC1yc2EAAAABIwAAAIEAudGEIaPARsKoVJVjs8XALAKqBN1WmXnY
kUf5oZjGY3QoMGDvNipQvdN3YmwLUBiKk31WvVwFB3N2K5a7fUBjoblkdjns
QKTKZiu4V+IL5rds/bD6LOEkJbjUzOjmp9hlIkh9uc0ceZ3ZxMtKhnORLrXL
aRyxYszO5FuirTo6xW8=
---- END SSH2 PUBLIC KEY ----
Public Key Fingerprint: 84:f8:24:db:74:9c:2d:51:06:0a:61:ef:82:13:88:88
```

Example 2. The following example displays the authentication method and DSA private key in encrypted format:

```
switchxxxxxx# show ip ssh-client key DSA
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
Authentication method: DSA key
Username: john
Key Source: User Defined
Public Key Fingerprint: 77:C7:19:85:98:19:27:96:C9:CC:83:C5:78:89:F8:86
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnDIaBDHtblQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
YI14Om1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
J0/RHd+NjB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1vO+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GDlB3VVmxHLmxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV ---- END SSH2 PUBLIC KEY ----
---- BEGIN SSH2 PRIVATE KEY ----
Comment: DSA Private Key
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnDIaBDHtblQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
YI14Om1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
J0/RHd+NjB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1vO+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GDlB3VVmxHLmxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV
---- END SSH2 PRIVATE KEY ----
```

Example 3. The following example displays the SSH client authentication method, the username and the password:

```
switchxxxxxx# show ip ssh-client Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
Authentication method: DSA key
Username: anonymous (default)
Password: anonymous (default)
password(Encrypted): KzGgzpYa7GzCHhaveSJDehGJ6L3Yf9ZBAU5nsxSxwic=
```

54.11. show ip ssh-client server

To display the SSH remote server authentication method and the Trusted Remote SSH Server table, use the `show ip ssh-client server` command in Privilege EXEC Configuration mode.

Syntax

- show ip ssh-client server [host | ip-address]

Parameters

- host - (Optional) DNS name of an SSH server.
- ip-address - (Optional) IP Address of an SSH server. The IP address can be an IPv4, IPv6 or IPv6 address. See IPv6 Address Conventions.

Default Configuration

None

Command Mode

Privileged EXEC mode

User Guidelines

If a specific SSH server is specified, only the fingerprint of this SSH server is displayed. Otherwise, all known servers are displayed.

Examples

Example 1 - In the following example, the SSH remote server authentication method and all trusted remote SSH servers are displayed:

```
switchxxxxxx# show ip ssh-client server SSH Server Authentication is enabled
server address: 11.1.0.1
 Server Key Fingerprint: 5a:8d:1d:b5:37:a4:16:46:23:59:eb:44:13:b9:33:e9 server
address: 192.165.204.111
 Server Key Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9 server
address: 4002:0011::12
 Server Key Fingerprint: a5:34:44:44:27:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

Example 2 - The following example displays the authentication method and DSA private key in encrypted format:

```
switchxxxxxx# show ip ssh-client key DSA
Authentication method: DSA key Username: john
Key Source: Default
Public Key Fingerprint: 77:C7:19:85:98:19:27:96:C9:CC:83:C5:78:89:F8:86
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnDIaBDHtblQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
YI14Om1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
J0/RHd+NjB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1vO+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GDlB3VVmxHLmxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV ---- END SSH2 PUBLIC KEY ----
---- BEGIN SSH2 PRIVATE KEY ----
Comment: DSA Private Key
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnDIaBDHtblQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
YI14Om1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
J0/RHd+NjB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
```

```
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1vO+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GDlB3VVmxHLmxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV
---- END SSH2 PRIVATE KEY ----
```

Example 3 - The following example displays the SSH client authentication method, the username and the password:

```
switchxxxxxx# show ip ssh-client
Authentication method: password (default) Username: anonymous (default)
password(Encrypted): KzGgzpYa7GzCHhaveSJDehGJ6L3Yf9ZBAU5
```

55. SYSLOG Commands

55.1. aaa logging

To enable logging AAA logins, use the `aaa logging` Global Configuration mode command. To disable logging AAA logins, use the no form of this command.

Syntax

- aaa logging {login}
- no aaa logging {login}

Parameters

- login - Enables logging messages related to successful AAA login events, unsuccessful AAA login events and other AAA login-related events.

Default Configuration

Enabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables logging messages related to successful login events, unsuccessful login events and other login-related events. Other types of AAA events are not subject to this command.

Example

The following example enables logging AAA login events.

```
switchxxxxxx(config)# aaa logging login
```

55.2. clear logging

To clear messages from the internal logging buffer, use the `clear logging` Privileged EXEC mode command.

Syntax

- clear logging

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example clears messages from the internal logging buffer.

```
switchxxxxxx# clear logging
Clear Logging Buffer ? (Y/N)[N]
```

55.3. clear logging file

To clear messages from the logging file, use the `clear logging file` Privileged EXEC mode command.

Syntax

- clear logging file

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example clears messages from the logging file.

```
switchxxxxxx# clear logging file
Clear Logging File [y/n]
```

55.4. file-system logging

To enable logging file system events, use the `file-system logging` Global Configuration mode command. To disable logging file system events, use the no form of this command.

Syntax

- file-system logging {copy | delete-rename}
- no file-system logging {copy | delete-rename}

Parameters

- copy - Specifies logging messages related to file copy operations.
- delete-rename - Specifies logging messages related to file deletion and renaming operations.

Default Configuration

Enabled.

Command Mode

Global Configuration mode

Example

The following example enables logging messages related to file copy operations.

```
switchxxxxxx(config)# file-system logging copy
```

55.5. logging buffered

To limit the SYSLOG message display to messages with a specific severity level, and to define the buffer size (number of messages that can be stored), use the `logging buffered` Global Configuration mode command. To cancel displaying the SYSLOG messages, and to return the buffer size to default, use the no form of this command.

Syntax

- logging buffered [buffer-size] [severity-level | severity-level-name]
- no logging buffered

Parameters

- buffer-size - (Optional) Specifies the maximum number of messages stored in buffer. (Range: 20–1000)
- severity-level - (Optional) Specifies the severity level of messages logged in the buffer. The possible values are: 1-7.
- severity-level-name - (Optional) Specifies the severity level of messages logged in the buffer. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

Default Configuration

The default severity level is informational.

The default buffer size is 1000.

Command Mode

Global Configuration mode

User Guidelines

All the SYSLOG messages are logged to the internal buffer. This command limits the messages displayed to the user.

Example

The following example shows two ways of limiting the SYSLOG message display from an internal buffer to messages with severity level debugging. In the second example, the buffer size is set to 100 and severity level informational.

```
switchxxxxxx(config)# logging buffered debugging
switchxxxxxx(config)# logging buffered 100 informational
```

55.6. logging console

To limit messages logged to the console to messages to a specific severity level, use the `logging console` Global Configuration mode command. To restore the default, use the no form of this command.

Syntax

- logging console level
- no logging console

Parameters

- level - Specifies the severity level of logged messages displayed on the console. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

Default Configuration

Informational.

Command Mode

Global Configuration mode

Example

The following example limits logging messages displayed on the console to messages with severity level errors.

```
switchxxxxxx(config)# logging console errors
```

55.7. logging file

To limit SYSLOG messages sent to the logging file to messages with a specific severity level, use the `logging file` Global Configuration mode command. To cancel sending messages to the file, use the no form of this command.

Syntax

- logging file level
- no logging file

Parameters

- level - Specifies the severity level of SYSLOG messages sent to the logging file. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

Default Configuration

The default severity level is errors.

Command Mode

Global Configuration mode

Example

The following example limits SYSLOG messages sent to the logging file to messages with severity level alerts.

```
switchxxxxxx(config)# logging file alerts
```

55.8. logging host

To log messages to the specified SYSLOG server, use the `logging host` Global Configuration command. To delete the SYSLOG server with the specified address from the list of SYSLOG servers, use the no form of this command.

Syntax

- logging host {ip-address | ipv6-address | hostname} [port port] [severity level] [facility facility] [description text]
- no logging host {ipv4-address | ipv6-address | hostname}

Parameters

- ip-address - IP address of the host to be used as a SYSLOG server. The IP address can be an IPv4, IPv6 or IPv6 address. See `IPv6 Address Conventions`.
- hostname - Hostname of the host to be used as a SYSLOG server. Only translation to IPv4 addresses is supported. (Range: 1–158 characters. Maximum label size for each part of the host name: 63)
- port port - (Optional) Port number for SYSLOG messages. If unspecified, the port number defaults to 514. (Range: 1–65535)

- severity level - (Optional) Limits the logging of messages to the SYSLOG servers to a specified level: Emergencies, Alerts, Critical, Errors, Warnings, Notifications, Informational, Debugging.
- facility facility - (Optional) The facility that is indicated in the message. It can be one of the following values: local0, local1, local2, local3, local4, local5, local 6, local7. If unspecified, the port number defaults to local7.
- description text - (Optional) Description of the SYSLOG server. (Range: Up to 64 characters)

Default Configuration

No messages are logged to a SYSLOG server.

If unspecified, the severity level defaults to Informational.

Command Mode

Global Configuration mode

User Guidelines

You can use up to 8 SYSLOG servers

Examples

```
switchxxxxxx(config)# logging host 1.1.1.121
switchxxxxxx(config)# logging host 3000::100/SYSLOG1
```

55.9. logging on

To enable message logging, use the `logging on` Global Configuration mode command. This command sends debug or error messages asynchronously to designated locations. To disable the logging, use the no form of this command.

Syntax

- logging on
- no logging on

Parameters

This command has no arguments or keywords.

Default Configuration

Message logging is enabled.

Command Mode

Global Configuration mode

User Guidelines

The logging process controls the logging messages distribution at various destinations, such as the logging buffer, logging file or SYSLOG server. Logging on and off at these destinations can be individually configured using the `clear logging file`, `logging console`, and `aaa logging` Global Configuration mode commands. However, if the `aaa logging` command is disabled, no messages are sent to these destinations. Only the console receives messages.

The following example enables logging error messages.

```
switchxxxxxx(config)# logging on
```

55.10. logging source-interface

To specify the source interface whose IPv4 address will be used as the source IPv4 address for communication with IPv4 SYSLOG servers, use the `logging source-interface` Global Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- logging source-interface interface-id
- no logging source-interface

Parameters

- interface-id - Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the interface IP address belonging to the next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface, the lowest IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 SYSLOG server.

OOB cannot be defined as a source interface.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# logging source-interface vlan 100
```

55.11. logging source-interface-ipv6

To specify the source interface whose IPv6 address will be used as the source IPv6 address for communication with IPv6 SYSLOG servers, use the `logging source-interface-ipv6` Global Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- logging source-interface-ipv6 interface-id
- no logging source-interface-ipv6

Parameters

- interface-id - Specifies the source interface.

Default Configuration

The IPv6 source address is the defined IPv6 address of the outgoing interface and selected in accordance with RFC6724.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

If the source interface is not the outgoing interface, the minimal IPv6 address defined on the source interface with the scope of the destination IPv6 address is applied.

If there is no available IPv6 source address, a SYSLOG message is issued when attempting to communicate with an IPv6 SYSLOG server.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# logging source-interface-ipv6 vlan 100
```

55.12. logging aggregation on

To control aggregation of SYSLOG messages, use the `logging aggregation on` Global Configuration mode command. If aggregation is enabled, logging messages are displayed every time interval (according to the aging time specified by `logging aggregation aging-time`). To disable aggregation of SYSLOG messages, use the no form of this command.

Syntax

- logging aggregation on
- no logging aggregation on

Parameters

This command has no arguments or keywords.

Default Configuration

Disabled

Command Mode

Global Configuration mode

Example

To turn off aggregation of SYSLOG messages:

```
switchxxxxxx(config)# no logging aggregation on
```

55.13. logging aggregation aging-time

To configure the aging time of the aggregated SYSLOG messages, use the `logging aggregation aging-time` Global Configuration mode command. The SYSLOG messages are aggregated during the time interval set by the aging-time parameter. To return to the default, use the no form of this command.

Syntax

- logging aggregation aging-time sec
- no logging aggregation aging-time

Parameters

- aging-time sec - Aging time in seconds (Range: 15–3600)

Default Configuration

300 seconds.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# logging aggregation aging-time 300
```

55.14. logging origin-id

To configure the origin field of the SYSLOG message packet headers sent to the SYSLOG server, use the `logging origin-id` Global Configuration mode command. To return to the default, use the no form of this command.

Syntax

- logging origin-id {hostname | IP | IPv6 | string user-defined-id}
- no logging origin-id

Parameters

- hostname - The system hostname will be used as the message origin identifier.
- IP - IP address of the sending interface that is used as the message origin identifier.
- IPv6 - IPv6 address of the sending interface that is used as the message origin identifier. If the sending interface is IPv4, the IPv4 address will be used instead.
- string user-defined-id - Specifies an identifying description chosen by the user. The user-defined-id argument is the identifying description string.

Default Configuration

No header is sent apart from the PRI field.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# logging origin-id string “Domain 1, router B”
```

55.15. show logging

To display the logging status and SYSLOG messages stored in the internal buffer, use the `show logging` Privileged EXEC mode command.

Syntax

- show logging

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example displays the logging status and the SYSLOG messages stored in the internal buffer.

```
switchxxxxxx# show logging
Logging is enabled. Origin id: hostname
Console Logging: Level info. Console Messages: 0 Dropped.
Buffer Logging: Level info. Buffer Messages: 61 Logged, 61 Displayed, 200 Max.
File Logging: Level error. File Messages: 898 Logged, 64 Dropped.
4 messages were not logged
Application filtering control
Application Event Status
------------------- ---------------- ---------
AAA Login Enabled
File system Copy Enabled
File system Delete-Rename Enabled Management ACL Deny Enabled
Aggregation: Disabled.
Aggregation aging time: 300 Sec
01-Jan-2010 05:29:46 :%INIT-I-Startup: Warm Startup
01-Jan-2010 05:29:02 :%LINK-I-Up: Vlan 1
01-Jan-2010 05:29:02 :%LINK-I-Up: SYSLOG6
01-Jan-2010 05:29:02 :%LINK-I-Up: SYSLOG7
01-Jan-2010 05:29:00 :%LINK-W-Down: SYSLOG8
```

55.16. show logging file

To display the logging status and the SYSLOG messages stored in the logging file, use the `show logging file` Privileged EXEC mode command.

Syntax

- show logging file

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example displays the logging status and the SYSLOG messages stored in the logging file.

```
switchxxxxxx# show logging file
Logging is enabled. Origin id: hostname
Console Logging: Level info. Console Messages: 0 Dropped.
Buffer Logging: Level info. Buffer Messages: 61 Logged, 61 Displayed, 200 Max.
File Logging: Level error. File Messages: 898 Logged, 64 Dropped.
4 messages were not logged
Application filtering control
```

```
Application Event Status
------------------- ---------------- ---------
AAA Login Enabled
File system Copy Enabled
File system Delete-Rename Enabled Management ACL Deny Enabled
Aggregation: Disabled.
Aggregation aging time: 300 Sec
1-Jan-2010 05:57:00 :%SSHD-E-ERROR: SSH error: key_read: type mismatch: encoding
error
01-Jan-2010 05:56:36 :%SSHD-E-ERROR: SSH error: key_read: type mismatch:
encoding error
01-Jan-2010 05:55:37 :%SSHD-E-ERROR: SSH error: key_read: type mismatch:
encoding error
01-Jan-2010 05:55:03 :%SSHD-E-ERROR: SSH error: key_read: key_from_blob bgEgGnt9
z6NHgZwKI5xKqF7cBtdl1xmFgSEWuDhho5UedydAjVkKS5XR2... failed
01-Jan-2010 05:55:03 :%SSHD-E-ERROR: SSH error: key_from_blob: invalid key type.
01-Jan-2010 05:56:34 :%SSHD-E-ERROR: SSH error: bad sigbloblen 58 != SIGBLOB_LEN
console#
```

55.17. show syslog-servers

To display the SYSLOG server settings, use the `show syslog-servers` Privileged EXEC mode command.

Syntax

- show syslog-servers

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example provides information about the SYSLOG servers.

```
switchxxxxxx# show syslog-servers Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
Device Configuration
--------------------
IP address Port Facility Severity Description
------------ ---- --------- -------- --------------
1.1.1.121 514 local7 info
3000::100 514 local7 info
OOB host Configuration
----------------------
IP address Port Facility Severity Description
------------ ---- --------- -------- --------------
2.1.1.200 514 local7 warning
```

56. System Management Commands

56.1. clear cpu counters

To clear traffic counters to and from the CPU, use the `clear cpu counters` EXEC mode command.

Syntax

- clear cpu counters

Parameters

This command has no arguments or keywords.

Default Usage

None

Command Mode

User EXEC mode

Example

The following example clears the CPU traffic counters.

```
switchxxxxxx> clear cpu counters
```

56.2. disable ports leds

To turn off the LEDs on all ports on a device, use the `disable ports` leds Global Configuration mode command.

To set the LEDs of all the ports on the device to their current operational status of the port, use the no disable ports leds command.

Syntax

- disable ports leds
- no disable ports leds

Parameters

This command has no arguments or keywords.

Default Configuration

The default is `no disable ports leds`; that is the LEDs of all the ports reflect their current status.

Command Mode

Global Configuration mode

Examples

```
The following example turns off the port LEDs.
switchxxxxxx(config)# disable ports leds
```

56.3. hostname

To specify or modify the device host name, use the `hostname` Global Configuration mode command. To remove the existing host name, use the no form of the command.

Syntax

- hostname name
- no hostname

Parameters

- Name - Specifies the device host name. (Length: 1-160 characters).

Default Configuration

No host name is defined.

Command Mode

Global Configuration mode

Example

The following example specifies the device host name as 'enterprise'.

```
switchxxxxxx(config)# hostname enterprise enterprise(config)#
```

56.4. reload

To reload the operating system at a user-specified time, use the `reload` Privileged EXEC mode command.

Syntax

- reload [in [hhh:mm | mmm] | at hh:mm [day month]] | cancel]

Parameters

- in hhh:mm | mmm - (Optional) Schedules a reload of the software to take effect in the specified minutes or hours and minutes. The reload must take place within approximately 24 days.
- at hh:mm - (Optional) Schedules a reload of the software to take place at the specified time (using a 24-hour clock). 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 (if the specified time is later than the current time) or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within 24 days.
- day - (Optional) Number of the day in the range from 1 to 31.
- month - (Optional) Month of the year.
- cancel - (Optional) Cancels a scheduled reload.

Default Usage

None

Command Mode

Privileged EXEC mode

User Guidelines

The at keyword can be used only if the system clock has been set on the device. To schedule reloads across several devices to occur simultaneously, synchronize the time on each device with SNTP.

When you specify the reload time using the at keyword, if you specify the month and day, the reload takes 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 (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within 24 days.

To display information about a scheduled reload, use the show reload command.

Examples

Example 1: The following example reloads the operating system.

```
switchxxxxxx> reload
This command will reset the whole system and disconnect your current session.
Do you want to continue? (y/n) [Y]
```

Example 2: The following example reloads the operating system in 10 minutes.

```
switchxxxxxx> reload in 10
This command will reset the whole system and disconnect your current session.
Reload is scheduled for 11:57:08 UTC Fri Apr 21 2012 (in 10 minutes). Do you
want to continue? (y/n) [Y]
```

Example 3: The following example reloads the operating system at 13:00.

```
switchxxxxxx> reload at 13:00
This command will reset the whole system and disconnect your current session.
Reload is scheduled for 13:00:00 UTC Fri Apr 21 2012 (in 1 hour and 3 minutes).
Do you want to continue? (y/n) [Y]
```

Example 4: The following example cancels a reload.

```
switchxxxxxx> reload cancel Reload cancelled.
```

56.5. resume

To enable switching to another open Telnet session, use the `resume` EXEC mode command.

Syntax

- resume [connection]

Parameters

- connection - (Optional) Specifies the connection number. (Range: 1-4 connections.)

Default Configuration

The default connection number is that of the most recent connection.

Command Mode

Privileged EXEC mode

Example

The following command switches to open Telnet session number 1.

```
switchxxxxxx> resume 1
```

56.6. service cpu-counters

To enable traffic counting to and from the CPU, use the `service cpu-counters` Global Configuration mode command. To disable counting, use the no form of this command.

Syntax

- service cpu-counters
- no service cpu-counters

Parameters

This command has no arguments or keywords.

Default Usage

None

Command Mode

Global Configuration mode

User Guidelines

Use the show cpu counters command to display the CPU traffic counters.

Example

The following example enables counting CPU traffic.

```
switchxxxxxx(config)# service cpu-counters
```

56.7. service cpu-utilization

To enable measuring CPU utilization, use the `service cpu-utilization` Global Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- service cpu-utilization
- no service cpu-utilization

Parameters

This command has no arguments or keywords.

Default Configuration

Measuring CPU utilization is enabled.

Command Mode

Global Configuration mode

User Guidelines

Use the service cpu utilization command to measure information on CPU utilization.

Example

The following example enables measuring CPU utilization.

```
switchxxxxxx(config)# service cpu-utilization
```

56.8. show cpu input rate

To display the rate of input frames to the CPU in packets per seconds (pps), use the `show cpu input rate` EXEC mode command.

Syntax

- show cpu input rate

Parameters

This command has no arguments or keywords.

Command Mode

User EXEC mode

Example

The following example displays CPU input rate information.

```
switchxxxxxx> show cpu input rate
Input Rate to CPU is 1030 pps.
```

56.9. show cpu utilization

To display information about CPU utilization, use the `show cpu utilization` Privileged EXEC mode command.

Syntax

```
show cpu utilization
```

Parameters

This command has no arguments or keywords.

Default Usage

None

Command Mode

Privileged EXEC mode

User Guidelines

Use the show cpu-utilization command to enable measuring CPU utilization.

Example

The following example displays CPU utilization information.

```
switchxxxxxx> show cpu utilization CPU utilization service is on.
CPU utilization
-----------------------------------------------
five seconds: 5%; one minute: 3%; five minutes: 3%
```

56.10. show cpu counters

To display traffic counter information to and from the CPU, use the `show cpu counters` EXEC mode command.

Syntax

- show cpu counters

Parameters

This command has no arguments or keywords.

Default Usage

None

Command Mode

User EXEC mode

User Guidelines

Use the service cpu-counters command to enable traffic counting to and from the CPU.

Example

The following example displays the CPU traffic counters.

```
switchxxxxxx> show cpu counters CPU counters are active.
In Octets: 987891
In Unicast Packets: 3589
In Multicast Packets: 29
In Broadcast Packets: 8
Out Octets: 972181
Out Unicast Packets: 3322
Out Multicast Packets: 22
Out Broadcast Packets: 8
```

56.11. show environment

To display environment information, use the `show environment` EXEC mode command.

Syntax

- show environment {all | fan | temperature {status} }

Parameters

- all - Displays the fan and temperature general status
- fan - Displays the fan status
- temperature status - Displays the temperature status

Command Mode

User EXEC mode

User Guidelines

The power parameters displays power supply information.

Main Power supply statuses:

- Active - power supply is used.
- Failure - Main power has failed.

The fan and temperature status parameters are available only on devices on which FAN and/or temperature sensor are installed.

Fan status can be one of:

- OK - The fan/s functions correctly.
- Failure - The fan failed.
- NA - No fan is installed.

Sensor status can be one of:

- OK - The sensor/s functions correctly.
- Failure - The sensor/s failed.
- NA - No sensor is installed.

Temperature can be one of:

- OK - The temperature is below the warning threshold.
- Warning- The temperature is between the warning threshold to the critical threshold.
- Critical - the temperature is above the critical threshold.

Examples

Example 1 - The following example displays the general environment status of a device.

```
switchxxxxxx> show environment all
Internal power supply Active.
.FAN is OK
TEMPERATURE is OK
```

Example 2 - The following example displays the power status of a device.

```
Internal power supply Active.
```

Example 2 - The following example displays the general FAN status of a device.

```
switchxxxxxx> show environment fan
FAN is OK
```

Example 3 - The following example displays the detailed temperature status of a device.

```
switchxxxxxx> show environment temperature status
TEMPERATURE is Warning
```

56.12. show inventory

To display system information, use the `show inventory` EXEC mode command.

Syntax

- show inventory [entity]

Parameters

- entity - Specifies the entity to be displayed. It can be a number (1 - 1) for a specific unit number, or an interface (Ethernet) name.

Command Mode

User EXEC mode

Examples

Example 1 - The following example displays all the entities in a standalone system.

```
switchxxxxxx> show inventory
NAME: "1", DESCR: "Ruggedized 24x1G_PoE+ 4x10G_SFP+ Microsens Managed Switch"
```

```
PID: Microsens, VID: V01, SN: 123456789
```

Example 2 - The following example displays a specific entity in a standalone system.

```
switchxxxxxx> show inventory 1
NAME: "1", DESCR: "Ruggedized 24x1G_PoE+ 4x10G_SFP+ Microsens Managed Switch"
PID: Microsens, VID: V01, SN: 123456789
```

56.13. show reload

To display whether there is a pending reload for status of the device, use the `show reload` Privileged EXEC mode command.

Syntax

- show reload

Parameters

This command has no arguments or keywords.

Default Usage

None

Command Mode

Privileged EXEC mode

User Guidelines

You can use this command to display a pending software reload. To cancel a pending reload, use this command with the cancel parameter.

Example

The following example displays that reboot is scheduled for 00:00 on Saturday, April-20.

```
switchxxxxxx> show reload
Reload scheduled for 00:00:00 UTC Sat April 20 (in 3 hours and 12 minutes)
```

56.14. show sessions

To display open Telnet sessions, use the `show sessions` EXEC mode command.

Syntax

- show sessions

Parameters

This command has no arguments or keywords.

Default Usage

None

Command Mode User EXEC mode User Guidelines

The show sessions command displays Telnet sessions to remote hosts opened by the current Telnet session to the local device. It does not display Telnet sessions to remote hosts opened by other Telnet sessions to the local device.

Example

The following example displays open Telnet sessions.

```
switchxxxxxx> show sessions
      Connection  Host  Address     Port  Byte
      ----------  ------------     ---------- ----- ----
Remote router     172.16.1.1 23     89
172.16.172.16.1.2 23    8
```

The following table describes significant fields shown above.

Field	Description
Connection	The connection number.
Host	The remote host to which the device is connected through a Telnet session.
Address	The remote host IP address.
Port	The Telnet TCP port number.
Byte	The number of unread bytes for the user to see on the connection.

56.15. show system

The show system EXEC mode command displays system information.

Syntax

- show system

Command Mode

User EXEC mode

Example

```
switchxxxxxx> show system
System Description:                         Microsens
System Up Time (days,hour:min:sec):         03,02:27:46
System Contact:
System Name:
System Location:
System MAC Address:                         00:60:a7:08:b0:fb
System Object ID:                           1.3.6.1.4.1.3181.1.20
Unit      Type
---- -----------------
 1      Microsens
Unit Temperature (Celsius)   Status
---- --------------------- ----------
 1            51               OK
```

56.16. show system languages

To display the list of supported languages, use the `show system languages` EXEC mode command.

Syntax

- show system languages

Parameters

This command has no arguments or keywords.

Default Usage

None

Command Mode

User EXEC mode

Example

The following example displays the languages configured on the device. Number of Sections indicates the number of languages permitted on the device.

```
switchxxxxxx> show system languages
 Language Name Unicode Name Code Num of Sections
--------------- -------------- ------ -------------
 English English en-US 2
 Japanese µùÑµ£¼F¬P ja-JP 2
```

56.17. show system tcam utilization

To display the Ternary Content Addressable Memory (TCAM) utilization, use the `show system tcam utilization` EXEC mode command.

Syntax

- show system tcam utilization [unit-id]

Parameters

- unit-id - (Optional) Specifies the unit number. (Range: 1–1)

Default Usage

None

Command Mode

User EXEC mode

Example

The following example displays TCAM utilization information.

```
switchxxxxxx> show system tcam utilization
TCAM utilization: 58%
```

56.18. show services tcp-udp

To display information about the active TCP and UDP services, use the `show services tcp-udp` Privileged EXEC mode command.

Syntax

- show services tcp-udp

Parameters

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

User Guidelines

The output does not show sessions where the device is a TCP/UDP client

Examples

```
switchxxxxxx> show services tcp-udp
Type Local IP Address Remote IP address Service Name State
-------------------- ------------------ ------------ -----------
TCP All:22 SSH LISTEN
TCP All:23 Telnet LISTEN
TCP All:80 HTTP LISTEN
TCP All:443 HTTPS ESTABLISHED
TCP 172.16.1.1:23 172.16.1.18:8789 Telnet
TCP6 All-23 Telnet LISTEN
TCP6 fe80::200:b0ff:fe00:0-23 Telnet
 fe80::200:b0ff:fe00:0-8999 ESTABLISHED
UDP All:161 SNMP
UDP6 All-161 SNMP
```

56.19. show tech-support

To display system and configuration information that can be provided to the Technical Assistance Center when reporting a problem, use the `show tech-support` EXEC mode command.

Syntax

- show tech-support [config | memory]

Parameters

- memory - (Optional) Displays memory and processor state data.
- config - (Optional) Displays switch configuration within the CLI commands supported on the device.

Default Configuration

By default, this command displays the output of technical-support-related show commands. Use keywords to specify the type of information to be displayed. If you do not specify any parameters, the system displays all configuration and memory data.

Command Types

Switch command.

Command Mode

User EXEC mode

User Guidelines

Caution: Avoid running multiple show tech-support commands on a switch or multiple switches on the network segment. Doing so may cause starvation of some time sensitive protocols, like STP.

The show tech-support command may time out if the configuration file output takes longer to display than the configured session time out time. If this happens, enter a set logout timeout value of 0 to disable automatic disconnection of idle sessions or enter a longer timeout value.

The show tech-support command output is continuous, meaning that it does not display one screen at a time. To interrupt the output, press Esc.

If the user specifies the memory keyword, the show tech-support command displays the following output:

- Flash info (dir if exists, or flash mapping)
- Output of command show bootvar
- Buffers info (like print os buff)
- Memory info (like print os mem)
- Proc info (like print OS tasks)
- Versions of software components
- Output of command show cpu utilization

56.20. show system fans

To view the status of the fans on the device, use the `show system fans` EXEC mode command.

Syntax

- show system fans

Command Mode

User EXEC mode

Examples

Example 1: For devices whose hardware supports variable fan speed.

```
switchxxxxxx> show system fans
      Unit Speed   State  (RPM)
--- --------- ------------------
      1       8000  Fans OK
```

56.21. show system sensors

To view the temperature sensor status, use the `show system sensors` EXEC mode command.

Syntax

- show system sensors

Parameters

This command has no arguments or keywords.

Default Usage

None

Command Mode

User EXEC mode

Examples

Example: The example displays device temperature information.

```
switchxxxxxx> show system sensor
Temperature Sensor Type Current Temperature (C) Target Temperature (C)
----------------------- ----------------------- -----------------------
Ambient1 47 60
Component 1 51 60
Component 2 52 60
Component 3 51 60
Component 4 51 60
```

56.22. show system id

To display the system identity information, use the `show system id` EXEC mode command.

Syntax

- show system id

Command Mode

User EXEC mode

Example

The following example displays the system identity information.

```
switchxxxxxx> show system id serial number 114
```

56.23. show ports leds configuration

To display whether the LEDs of the ports are enabled or disabled, use the `show port leds configuration` EXEC mode command.

Syntax

- show ports leds configuration

Parameters

This command has no arguments or keywords.

Command Mode

User EXEC mode

Examples

Example 1: The following example displays the status of the port's LEDs when they are turned on.

```
switchxxxxxx> show ports leds configuration
Port leds are not disabled
```

Example 2: The following example displays the status of the port LEDs when they are turned off.

```
switchxxxxxx> show port leds configuration
Port leds are disabled
```

56.24. show users

To display information about the active users, use the `show users` EXEC mode command.

Syntax

- show users

Parameters

This command has no arguments or keywords.

Default Usage

None

Command Mode

User EXEC mode

Example

The following example displays information about the active users.

```
switchxxxxxx> show users
Username Protocol Location
-------- -------- --------
Bob Serial 172.16.0.1
John SSH 172.16.0.8
Robert HTTP 172.16.1.7
Betty Telnet 172.16.1.6
```

56.25. show version

To display system version information, use the `show version` EXEC mode command.

Syntax

- show version

Command Mode

User EXEC mode

Example

The following example displays system version information.

```
switchxxxxxx> show version
SW Version 1.1.0.5 ( date 15-Sep-2010 time 10:31:33 )
Boot Version 1.1.0.2 ( date 04-Sep-2010 time 21:51:53 )
HW Version
```

56.26. show hardware version

To display hardware version information, use the `show hardware version` EXEC mode command.

Syntax

- show hardware version

Command Mode

User EXEC mode

Example

The following example displays hardware version information.

```
switchxxxxxx> show hardware version
Hardware Version 1.0.0
```

56.27. system recovery

To set the system to automatically recover from temperature that reached the critical threshold, use the `system recovery` Global Configuration command.

To return to disable automatic recovery, use the no form of the command.

Syntax

- system recovery
- no system recovery

Parameters

This command has no arguments or keywords.

Default Configuration

System recovery is enabled by default.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# no system recovery
```

57. UDLD Commands

57.1. show udld

To display the administrative and operational Unidirectional Link Detection Protocol (UDLD) status, use the `show udld` command in Privileged EXEC mode.

Syntax

- show udld [interface-id] [neighbors]

Parameters

- interface-id - Interface identifier of an Ethernet port.
- neighbors - Displays neighbor information only.

Command Mode

Privileged EXEC mode

User Guidelines

If you do not enter an interface ID value, the administrative and operational UDLD status for all interfaces on which UDLD is enabled are displayed.

Examples

Example 1: This example shows how to display the UDLD state for all interfaces. Most of the fields shown in the display are self-explanatory. Those that are not self-explanatory are defined below.

```
switchxxxxxx# show udld
Global UDLD mode: normal
Message Time: 15 sec(default)
Interface te1/0/1
  Port UDLD mode: aggressive
  Port Current state: Bidirectional
  Number of detected neighbors: 1
  Port Neighbor Table
    Neighbor Device ID: 1234567893
      Neighbor MAC: 00:00:01:22:33:dd
      Neighbor Device name: switch A
      Neighbor Port ID: gi1/2/1
      Neighbor Message Time: 20 sec
      Neighbor Current State: Bidirectional
      Neighbor Expiration Time: 7 sec
    Neighbor Device ID: 1234544893
      Neighbor MAC: 00:00:01:22:33:ff
      Neighbor Device name: switch A
      Neighbor Port ID: gi1/2/1
      Neighbor Message Time: 15 sec
      Neighbor Current State: Undetermined
      Neighbor Expiration Time: 17 sec
Interface te1/0/2
  Port UDLD mode: normal (default)
  Port Current state: Undetermined
  Number of detected neighbors: 1
    Neighbor Device ID: 1234567753
      Neighbor MAC: 00:00:01:22:33:fe
```

```
      Neighbor Device name: switch A
      Neighbor Port ID: gi1/2/1
      Neighbor Message Time: 15 sec
      Neighbor Current State: Undetermined
      Neighbor Expiration Time: 11 sec
Interface te1/0/3
  Port UDLD mode: disabled
Interface te1/0/4
  Port UDLD mode: normal (default)
  Port Current state: shutdown
```

Field Descriptions:

- Global UDLD mode - The global UDLD mode (normal or aggressive) configured by the udld command.
- Message Time - The message time configured by the udld message time command.
- Port UDLD mode - The interface UDLD mode (normal or aggressive).
- Port Current state - The UDLD operational state: interface UDLD mode (normal or aggressive).
  - Disabled - UDLD is disabled on the port by the udld port disable command.
  - Shutdown - UDLD is enabled on the port and the port operational state is DOWN.
  - Detection - UDLD id detecting the link state.
  - Bidirectional - The link is bidirectional.
  - Undetermined - The link state is undetermined - no UDLD message has been received on the port.
- Neighbor Device ID - The device ID of the neighbor.
- Neighbor MAC - The MAC address of the neighbor.
- Neighbor Device name - The Device name of the neighbor.
- Neighbor Port ID - The device port ID of the neighbor on which the recent UDLD message was sent.
- Neighbor Message Time - The message time of the neighbor.
- Neighbor Current State - The current state of the neighbor:
  - Bidirectional - The UDLD messages received from the neighbor contain the Device ID and Port ID of the switch in the Echo TLV.
  - Undetermined - The UDLD messages received from the neighbor do not contain the Device ID and Port ID of the switch in the Echo TLV.
- Neighbor Expiration Time - Left time in seconds until the current neighbor state expires.

Example 2: This example shows how to display the UDLD state for one given interface:

```
switchxxxxxx# show udld te1/0/1
Global UDLD mode: normal
Message Time: 15 sec(default)
Interface te1/0/1
Port UDLD mode: aggressive
Port Current state: Bidirectional
Number of detected neighbors: 1
Port Neighbor Table
  Neighbor Device ID: 1234567893
    Neighbor MAC: 00:00:01:22:33:dd
    Neighbor Device name: switch A
    Neighbor Port ID: gi1/2/1
```

```
    Neighbor Message Time: 20 sec
    Neighbor Current State: Bidirectional
    Neighbor Expiration Time: 7 sec
  Neighbor Device ID: 1234544893
    Neighbor MAC: 00:00:01:22:33:ff
    Neighbor Device name: switch A
    Neighbor Port ID: gi1/2/1
    Neighbor Message Time: 15 sec
    Neighbor Current State: Undetermined
    Neighbor Expiration Time: 17 sec
```

Example 3: This example shows how to display neighbor information only:

```
switchxxxxxx# show udld neighbors
Port     Device ID      Port-ID   Device Name     Message  Neighbor   Expiration
                                                 Time(sec)State      Time (sec)
-------- -------------- --------- --------------- --------- ---------- ---------
te1/0/1  1234567893     gi1/0/1   SAL0734K5R2     15        Bidirect          11
te1/0/2  3456750193     gi1/0/2   SAL0734K5R3     20        Undetermined       5
```

Example 4: This example shows how to display neighbor information only for a single interface:

```
switchxxxxxx# show udld te1/0/1 neighbors
Port     Device ID      Port-ID   Device Name     Message  Neighbor   Expiration
                                                 Time(sec)State      Time (sec)
-------- -------------- --------- --------------- --------- ---------- ---------
te1/0/1  1234567893     gi1/0/1   SAL0734K5R2     15        Bidirect          11
```

57.2. udld

Use the `udld` command in Global Configuration mode to globally enable the UniDirectional Link Detection (UDLD) protocol. To disable UDLD, use the no form of this command.

Syntax

- udld aggressive | normal
- no udld

Parameters

- aggressive - Enables UDLD in aggressive mode by default on all fiber interfaces.
- normal - Enables UDLD in normal mode by default on all fiber interfaces.

Default Configuration

UDLD is disabled on all fiber interfaces.

Command Mode

Global Configuration mode

User Guidelines

This command affects fiber interfaces only. Use the `udld port` command in Interface Configuration mode to enable UDLD on other interface types. Use the no form of this command to disable UDLD on all fiber ports.

The device supports the UDLD protocol specified by RFC 5171.

UDLD supports two modes of operation: normal and aggressive. In the aggressive mode the device shuts down a port if it cannot explicitly detect that the link is bidirectional. In the normal mode the device shuts down an interface if it explicitly detect that the link is unidirectional. A unidirectional link occurs whenever traffic sent by a local device is received by its neighbor but traffic from the neighbor is not received by the local device.

You can use the following commands to reset an interface shut down by UDLD:

- The errdisable recover reset command with the interface interface-id parameter to reset a given interface.
- The errdisable recover reset command with the udld parameter to reset all interfaces shut down by UDLD.
- The errdisable recover cause with the udld parameter to automatically recover from the UDLD error-disabled state.

Example

This example shows how to enable UDLD on all fiber interfaces:

```
switchxxxxxx(config)# udld normal
```

57.3. udld message time

Use the `udld message time` command in Global Configuration mode to configure a global value of the interval between two sent probe messages. To return to the default value, use the no form of this command.

Syntax

- udld message time seconds
- no udld message time

Parameters

- seconds - Interval between two sent probe messages. The valid values are from 1 to 90 seconds.

Default Configuration

15 seconds.

Command Mode

Global Configuration mode

User Guidelines

Use this command to change the default value of the message interval – the interval between two sequential sent probe messages.

Example

This example shows how to globally set the interval to 40sec:

```
switchxxxxxx(config)# udld message time 40
```

57.4. udld port

To enable the UDLD protocol on an Ethernet port, use the `udld port` command in Interface Configuration mode. To return to the default, use the no form of this command.

Syntax

udld port [aggressive | normal | disable]

no udld port

Parameters

- aggressive - Enables UDLD in aggressive mode on this interface.
- normal - Enables UDLD in normal mode on this interface. The normal keyword is applied if no keyword is specified.
- disable - Disables UDLD on this interface.

Default Configuration

The defaults are as follows:

- Fiber interfaces are in the state configured by the `udld` command.
- Non-fiber interfaces are in the Disable state.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

Use this command on fiber ports to override the setting of the global `udld` command.

If the port changes from fiber to non-fiber or vice versa, all configurations are maintained because the platform software detects a change of module or a Gigabit Interface Converter (GBIC) change.

Examples

Example 1: This example shows how to enable UDLD in normal mode on an Ethernet port regardless of the current global udld setting:

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# udld port normal
switchxxxxxx(config-if)# exit
```

Example 2: This example shows how to return to the default configuration:

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# no udld port
switchxxxxxx(config-if)# exit
```

Example 3: This example shows how to disable UDLD on an Ethernet port regardless of the current global udld setting:

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# udld port disable
switchxxxxxx(config-if)# exit
```

58. User Interface Commands

58.1. banner exec

To specify and enable a message to be displayed after a successful logon, use the `banner exec` Global Configuration mode command. This banner is applied automatically on all the user interfaces: console, Telnet and SSH and also on the WEB GUI. To delete the existing EXEC banner, use the no form of this command.

Syntax

- banner exec d message-text d
- no banner exec

Parameters

- d - Delimiting character of user’s choice - a pound sign (#), for example. You cannot use the delimiting character in the banner message.
- message-text - The message must start in a new line. You can enter multi-line messages. You can include tokens in the form of $(token) in the message text. Tokens are replaced with the corresponding configuration variable (see User Guidelines). The message can contain up to 1000 characters (after every 510 characters, press <Enter> to continue).

Default Configuration

Disabled (no EXEC banner is displayed).

Command Mode

Global Configuration mode

User Guidelines

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

Use tokens in the form of $(token) in the message text to customize the banner. The tokens are described in the table below:

Token	Information Displayed in the Banner
$(hostname)	Displays the host name for the device.
$(domain)	Displays the domain name for the device.
$(bold)	Indicates that the next text is a bold text. Using this token again indicates the end of the bold text.
$(inverse)	Indicates that the next text is an inverse text. Using this token again indicates the end of the inverse text.
$(contact)	Displays the system contact string.
$(location)	Displays the system location string.
$(mac-address)	Displays the base MAC address of the device.

Use the no banner exec Line Configuration command to disable the Exec banner on a particular line or lines.

Example

The following example sets an EXEC banner that uses tokens. The percent sign (%) is used as a delimiting character. Note that the $(token) Syntax is replaced by the corresponding configuration variable.

```
switchxxxxxx(config)# banner exec %
Enter TEXT message. End with the character '%'.
$(bold)Session activated.$(bold) Enter commands at the prompt.
%
When a user logs on to the system, the following output is displayed:
Session activated. Enter commands at the prompt.
```

58.2. banner login

To specify a message to be displayed before the username and password login prompts, use the `banner login` command in Global Configuration mode. This banner is applied automatically on all the user interfaces: Console, Telnet and SSH and also on the WEB GUI. To delete the existing login banner, use the no form of this command

Syntax

- banner login d message-text d
- no banner login

Parameters

- d - Delimiting character of user's choice - a pound sign (#), for example. You cannot use the delimiting character in the banner message.
- message-text - Message text. The message must start on a new line. You can enter multi-line messages. You can include tokens in the form of $(token) in the message text. Tokens are replaced with the corresponding configuration variable (see User Guidelines). The message can contain up to 1000 characters (after every 510 characters, you must press <Enter> to continue).

Default Configuration

Disabled (no Login banner is displayed).

Command Mode

Global Configuration mode

User Guidelines

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

Use tokens in the form of $(token) in the message text to customize the banner. The tokens are described in the table below:

Token	Information displayed in the banner
$(hostname)	Displays the host name for the device.
$(domain)	Displays the domain name for the device.

$(bold)	Indicates that the next text is a bold text. Using this token again indicates the end of the bold text.
$(inverse)	Indicates that the next text is an inverse text. Using this token again indicates the end of the inverse text.
$(contact)	Displays the system contact string.
Token	Information displayed in the banner
$(location)	Displays the system location string.
$(mac-addre ss)	Displays the base MAC address of the device.

Use the no banner login Line Configuration command to disable the Login banner on a particular line or lines.

Example

The following example sets a Login banner that uses tokens. The percent sign (%) is used as a delimiting character. Note that the $(token) Syntaxis replaced by the corresponding configuration variable.

```
switchxxxxxx(config)# banner login %
Enter TEXT message. End with the character '%'.
You have entered $(hostname).$(domain)
%
When the login banner is executed, the user will see the following banner:
You have entered host123.ourdomain.com
```

58.3. configure

To enter the Global Configuration mode, use the `configure` Privileged EXEC mode command.

Syntax

- configure [terminal]

Parameters

- terminal - (Optional) Enter the Global Configuration mode with or without the keyword terminal.

Command Mode

Privileged EXEC mode

Example

The following example enters Global Configuration mode.

```
switchxxxxxx# configure
switchxxxxxx(config)#
```

58.4. disable

To leave the Privileged EXEC mode and return to the User EXEC mode, use the `disable` Privileged EXEC mode command.

Syntax

- disable [privilege-level]

Parameters

- privilege-level - (Optional) Reduces the privilege level to the specified privileged level. If privilege level is left blank, the level is reduce to the minimal privilege level.

Default Configuration

The default privilege level is 15.

Command Mode

Privileged EXEC mode

Example

The following example returns the user to user level 1.

```
switchxxxxxx# disable 1
switchxxxxxx#
```

58.5. do

To execute an EXEC-level command from Global Configuration mode or any configuration submode, use the `do` command.

Syntax

- do command

Parameters

- command - Specifies the EXEC-level command to execute.

Command Mode

All configuration modes

Example

The following example executes the show vlan Privileged EXEC mode command from Global Configuration mode.

```
switchxxxxxx(config)# do show vlan
Vlan Name Ports Type Authorization
---- ---- ----- ---- -------------
1 1 te1/0/1-4,Po1,Po2 other Required
2 2 te1/0/1 dynamicGvrp Required
10 v0010 te1/0/1 permanent Not Required
11 V0011 te1/0/1,te1/0/3 permanent Required
20 20 te1/0/1 permanent Required
30 30 te1/0/1,te1/0/3 permanent Required
31 31 te1/0/1 permanent Required
91 91 te1/0/1,te1/0/4 permanent Required
4093 guest-vlan te1/0/1,te1/0/3 permanent Guest
switchxxxxxx(config)#
```

58.6. enable

To enter the Privileged EXEC mode, use the `enable` User EXEC mode command.

Syntax

- enable [privilege-level]

Parameters

- privilege-level - (Optional) Specifies the privilege level at which to enter the system.(Range: 1,15)

Default Configuration

The default privilege level is 15.

Command Mode

User EXEC mode

Example

The following example enters privilege level 15.

```
switchxxxxxx# enable enter password:**********
switchxxxxxx# Accepted
```

58.7. end

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

Syntax

- end

Parameters

This command has no arguments or keywords

Default Configuration

None

Command Mode

All configuration modes

Example

The following example ends the Global Configuration mode session and returns to the Privileged EXEC mode.

```
switchxxxxxx(config)# end
switchxxxxxx#
```

58.8. exit (Configuration)

To exit any mode and bring the user to the next higher mode in the CLI mode hierarchy, use the `exit` command.

Syntax

- exit

Parameters

This command has no arguments or keywords

Default Configuration

None

Command Mode

All configuration modes

Examples

The following examples change the configuration mode from Interface Configuration mode to Privileged EXEC mode.

```
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# exit
```

58.9. exit (EXEC)

To close an active terminal session by logging off the device, use the `exit` User EXEC mode command.

Syntax

- exit

Parameters

This command has no arguments or keywords

Default Configuration

None

Command Mode

User EXEC mode

Example

The following example closes an active terminal session.

```
switchxxxxxx# exit
```

58.10. help

To display a brief description of the Help system, use the `help` command.

Syntax

- help

Parameters

This command has no arguments or keywords

Default Configuration

None

Command Mode

All configuration modes

Example

The following example describes the Help system.

```
switchxxxxxx# help
```

Help may be requested at any point in a command by entering a question mark '**?**'. If nothing matches the currently entered incomplete command, the help list is empty. This indicates that there is no command matching the input as it currently appears. If the request is within a command, press the Backspace key and erase the entered characters to a point where the request results in a match.

Help is provided when:

- There is a valid command and a help request is made for entering a parameter or argument (e.g. 'show ?'). All possible parameters or arguments for the entered command are then displayed.
- An abbreviated argument is entered and a help request is made for arguments matching the input (e.g. 'show pr?').

58.11. history

To enable saving commands that have been entered, use the `history` Line Configuration Mode command. To disable the command, use the no form of this command.

Syntax

- history
- no history

Parameters

This command has no arguments or keywords

Default Configuration

Enabled.

Command Mode

Line Configuration Mode

User Guidelines

This command enables saving user-entered commands for a specified line. You can return to previous lines by using the up or down arrows.

It is effective from the next time that the user logs in via console/telnet/ssh.

The following are related commands:

- Use the `terminal history size` User EXEC mode command to enable or disable this command for the current terminal session.
- Use the `history size` Line Configuration Mode command to set the size of the command history buffer.

Example

The following example enables the command for Telnet.

```
switchxxxxxx(config)# line telnet
switchxxxxxx(config-line)# history
```

58.12. history size

To change the maximum number of user commands that are saved in the history buffer for a particular line, use the `history size` Line Configuration Mode command. To reset the command history buffer size to the default value, use the no form of this command.

Syntax

- history size number-of-commands
- no history size

Parameters

- number-of-commands - Specifies the number of commands the system records in its history buffer.

Default Configuration

The default command history buffer size is 256 commands.

Command Mode

Line Configuration Mode

User Guidelines

This command configures the command history buffer size for a particular line. It is effective from the next time that the user logs in via console/telnet/ssh.

Use the terminal history size User EXEC mode command to configure the command history buffer size for the current terminal session.

The allocated command history buffer is per terminal user, and is taken from a shared buffer. If there is not enough space available in the shared buffer, the command history buffer size cannot be increased above the default size.

Example

The following example changes the command history buffer size to 100 entries for Telnet.

```
switchxxxxxx(config)# line telnet
switchxxxxxx(config-line)# history size 100
```

58.13. login

To enable changing the user that is logged in, use the `login` User EXEC mode command. When this command is logged in, the user is prompted for a username/password.

Syntax

- login

Parameters

This command has no arguments or keywords

Default Configuration

None

Command Mode

User EXEC mode

Example

The following example enters Privileged EXEC mode and logs in with the required username ‘bob’.

```
switchxxxxxx# login User Name:bob
Password:*****
switchxxxxxx#
```

58.14. terminal datadump

To enable dumping all the output of a show command without prompting, use the `terminal datadump` User EXEC mode command. To disable dumping, use the no form of this command.

Syntax

- terminal datadump
- no terminal datadump

Parameters

This command has no arguments or keywords

Default Configuration

When printing, dumping is disabled and printing is paused every 24 lines.

Command Mode

User EXEC mode

User Guidelines

By default, a `More` prompt is displayed when the output contains more than 24 lines. Pressing the Enter key displays the next line; pressing the Spacebar displays the next screen of output.

The terminal datadump command enables dumping all output immediately after entering the show command by removing the pause.

The width is not limited, and the width of the line being printed on the terminal is based on the terminal itself.

This command is relevant only for the current session.

Example

The following example dumps all output immediately after entering a show command.

```
switchxxxxxx# terminal datadump
```

58.15. terminal history

To enable the command history function for the current terminal session, meaning that it will not be stored in the Running Configuration file, use the `terminal history` User EXEC mode command. To disable the command, use the no form of this command.

Syntax

- terminal history
- no terminal history

Parameters

This command has no arguments or keywords

Default Configuration

The default configuration for all terminal sessions is defined by the `history` Line Configuration Mode command.

Command Mode

User EXEC mode

User Guidelines

The command enables the command history for the current session. The default is determined by the `history` Line Configuration Mode command.

This command is effective immediately.

Example

The following example disables the command history function for the current terminal session.

```
switchxxxxxx# terminal no history
```

58.16. terminal history size

To change the command history buffer size for the current terminal session, meaning it will not be stored in the Running Configuration file, use the `terminal history size` User EXEC mode command. , use the no form of this command to reset the command history buffer size to the default value.

Syntax

- terminal history size number-of-commands
- no terminal history size

Parameters

- number-of-commands - Specifies the number of commands the system maintains in its history buffer. (Range: 10–206)

Default Configuration

The default configuration for all terminal sessions is defined by the `history size` Line Configuration Mode command.

Command Mode

User EXEC mode

User Guidelines

The terminal history size EXEC command changes the command history buffer size for the current terminal session. Use the `history` Line Configuration Mode command to change the default history buffer size.

The maximum number of commands in all buffers is 207.

Example

The following example sets the command history buffer size to 20 commands for the current terminal session.

```
switchxxxxxx# terminal history size 20
```

58.17. terminal prompt

To enable the terminal prompts, use the `terminal prompt` User EXEC mode command. To disable the terminal prompts, use terminal no prompt command.

The command is per session and will not be saved in the configuration database.

Syntax

- terminal prompt
- no terminal prompt

Parameters

This command has no arguments or keywords

Default Configuration

The default configuration is prompts enabled.

Command Mode

Privileged EXEC mode

Example

The following example disables the terminal prompts

```
switchxxxxxx# terminal no prompt
```

58.18. terminal width

To determine the width of the display for the echo input to CLI sessions, use the `terminal width` User EXEC mode command. To return to the default, use terminal no width.

The command is per session and will not be saved in the configuration database.

Syntax

- terminal width number-of-characters
- no terminal width

Parameters

- number-of-characters - Specifies the number of characters to be displayed for the echo output of the CLI commands and the configuration file,'0' means endless number of characters on a screen line. (Range: 0, 70-512)

Default Configuration

The default number of characters is 77.

Command Mode

Privileged EXEC mode

Example

The following example sets the terminal width to 100 characters

```
switchxxxxxx# terminal width 100
```

58.19. show banner

To display the banners that have been defined, use the `show banner` commands in User EXEC mode.

Syntax

- show banner login
- show banner exec

Parameters

This command has no arguments or keywords

Command Mode

User EXEC mode

Examples

```
switchxxxxxx# show banner login
------------------------------------------------------------
Banner: Login
Line SSH: Enabled
Line Telnet: Enabled Line Console: Enabled
switchxxxxxx# show banner exec
Banner: EXEC
Line SSH: Enabled
Line Telnet: Enabled
Line Console: Enabled
You have logged on
```

58.20. show history

To list the commands entered in the current session, use the `show history` User EXEC mode command.

Syntax

- show history

Parameters

This command has no arguments or keywords

Default Configuration

None

Command Mode

User EXEC mode

User Guidelines

The buffer includes executed and unexecuted commands.

Commands are listed from the first to the most recent command.

The buffer remains unchanged when entering into and returning from configuration modes.

Example

The following example displays all the commands entered while in the current Privileged EXEC mode.

```
switchxxxxxx# show version
SW version 3.131 (date 23-Jul-2005 time 17:34:19) HW version 1.0.0
switchxxxxxx# show clock 15:29:03 Jun 17 2005
switchxxxxxx# show history show version show clock show history
3 commands were logged (buffer size is 10)
```

58.21. show privilege

To display the current privilege level, use the `show privilege` User EXEC mode command.

Syntax

- show privilege

Parameters

This command has no arguments or keywords

Default Configuration

None

Command Mode

User EXEC mode

Example

The following example displays the privilege level for the user logged on.

```
switchxxxxxx# show privilege
Current privilege level is 15
```

59. Virtual Local Area Network (VLAN) Commands

59.1. vlan database

Use the `vlan database` Global Configuration mode command to enter the VLAN Configuration mode. This mode is used to create VLAN(s) and define the default VLAN.

Use the `exit` command to return to Global Configuration mode.

Syntax

- vlan database

Parameters

N/A

Default Configuration

VLAN 1 exists by default.

Command Mode

Global Configuration mode

Example

The following example enters the VLAN Configuration mode, creates VLAN 1972 and exits VLAN Configuration mode.

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# vlan 1972
switchxxxxxx(config-vlan)# exit
```

59.2. vlan

Use the `vlan` VLAN Configuration mode or Global Configuration mode command to create a VLAN and assign it a name (if only a single VLAN is being created). Use the no form of this command to delete the VLAN(s).

Syntax

- vlan vlan-range | {vlan-id [name vlan-name]} [media ethernet] [state active]
- no vlan vlan-range

Parameters

- vlan-range - Specifies a list of VLAN IDs. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs (range: 2-4094).
- vlan-id - Specifies a VLAN ID. (range: 2-4094).
- vlan-name - Specifies the VLAN name. (range: 1–32 characters).
- media - Specifies the media type of the VLAN. Valid values are ethernet.
- state - Specifies whether the state of the VLAN. Valid values are active.

Default Configuration

VLAN 1 exists by default.

Command Mode

Global Configuration mode

VLAN Database Configuration mode

User Guidelines

If the VLAN does not exist, it is created. If the VLAN cannot be created then the command is finished with error and the current context is not changed.

Example

The following example creates a few VLANs. VLAN 1972 is assigned the name Marketing.

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# vlan 19-23
switchxxxxxx(config-vlan)# vlan 100
switchxxxxxx(config-vlan)# vlan 1972 name Marketing
switchxxxxxx(config-vlan)# exit
```

59.3. show vlan

Use the `show vlan` Privileged EXEC mode command to display the following VLAN information.

Syntax

- show vlan [tag vlan-id | name vlan-name]

Parameters

- tag vlan-id - Specifies a VLAN ID.
- name vlan-name - Specifies a VLAN name string (length: 1–32 characters)

Default Configuration

All VLANs are displayed.

Command Mode

Privileged EXEC mode

Examples

Example 1 - The following example displays information for all VLANs:

```
switchxxxxxx# show vlan
Created by: S-Static, G-GVRP, R-Radius Assigned VLAN, V-Voice VLAN
VLAN Name Tagged Ports UnTagged Ports Created by
---- --------- ------------ -------------- ----------
1 Default te1/0/1 S
10 Marketing te1/0/2 te1/0/2 S
91 11 te1/0/2-4 te1/0/2 SGR
 11 te1/0/3-4 G
 11 te1/0/3-4 GR
```

59.4. interface vlan

Use the `interface vlan` Global Configuration mode command to enter the Interface Configuration (VLAN) mode for a specific VLAN. After this command is entered, all commands configure this VLAN.

Syntax

- interface vlan vlan-id

Parameters

- vlan-id - Specifies the VLAN to be configured.

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

If the VLAN does not exist, the VLAN is created. If the VLAN cannot be created, this command is finished with an error and the current context is not changed.

Example

The following example configures VLAN 1 with IP address 131.108.1.27 and subnet mask 255.255.255.0.

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip address 131.108.1.27 255.255.255.0
```

59.5. interface range vlan

Use the `interface range vlan` Global Configuration mode command to configure multiple VLANs simultaneously.

Syntax

- interface range vlan vlan-range

Parameters

- vlan-range - Specifies a list of VLANs. Separate nonconsecutive VLANs with a comma and no spaces. Use a hyphen to designate a range of VLANs.

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

Commands under the interface VLAN range context are executed independently on each VLAN in the range. If the command returns an error on one of the VLANs, an error message is displayed, and the system attempts to configure the remaining VLANs.

Example

The following example groups VLANs 221 through 228 and 889 to receive the same command(s).

```
switchxxxxxx(config)# interface range vlan 221-228, vlan 889
```

59.6. name

Use the `name` Interface Configuration (VLAN) mode command to name a VLAN. Use the no form of this command to remove the VLAN name.

Syntax

- name string
- no name

Parameters

- string - Specifies a unique name associated with this VLAN. (Length: 1–32 characters).

Default Configuration

No name is defined.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

The VLAN name must be unique.

Example

The following example assigns VLAN 19 the name Marketing.

```
switchxxxxxx(config)# interface vlan 19
switchxxxxxx(config-if)# name Marketing
```

59.7. switchport protected-port

Use the `switchport protected-port` Interface Configuration mode command to isolate Unicast, Multicast, and Broadcast traffic at Layer 2 from other protected ports on the same switch. Use the no form of this command to disable protection on the port.

Syntax

- switchport protected-port
- no switchport protected-port

Parameters

N/A

Default Configuration

Unprotected

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Note that packets are subject to all filtering rules and Filtering Database (FDB) decisions.

Use this command to isolate Unicast, Multicast, and Broadcast traffic at Layer 2 from other protected ports (that are not associated with the same community as the ingress interface) on the same switch. Please note that the packet is still subject to FDB decision and to all filtering rules.

Use the `switchport community` Interface Configuration command to associate the interface with a community.

Example

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# switchport protected-port
```

59.8. show interfaces protected-ports

Use the `show interfaces protected-ports` EXEC mode command to display protected ports configuration.

Syntax

- show interfaces protected-ports [interface-id | detailed]

Parameters

- interface-id - Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- detailed - Displays information for non-present ports in addition to present ports.

Default Configuration

Show all protected interfaces. If detailed is not used, only present ports are displayed.

Command Mode

User EXEC mode

Example

```
switchxxxxxx# show interfaces protected-ports
Interface State Community
--------- ----------- ---------
te1/0/1 Protected 1
te1/0/2 Protected Isolated 20
te1/0/3 Unprotected Isolated
te1/0/4 Unprotected
```

59.9. switchport community

Use the `switchport community` Interface Configuration mode command to associate a protected port with a community. Use the no form of this command to return to the default.

Syntax

- switchport community community
- no switchport community

Parameters

- community - Specifies the community number. (range: 1 - 31).

Default Configuration

The port is not associated with a community.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The command is relevant only when the port is defined as a protected port. Use the `switchport protected-port` Interface Configuration command to define a port as a protected port.

Example

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# switchport community 1
```

59.10. switchport

Use the `switchport` Interface Configuration mode command to put an interface that is in Layer 3 mode into Layer 2 mode. Use the no form of this command to put an interface in Layer 3 mode.

Syntax

- switchport
- no switchport

Parameters

N/A

Default Configuration

Layer 2 mode

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use the no switchport command to set the interface as a Layer 3 interface.

An interface cannot be set as a Layer 3 interface if 802x.1 is enabled on the interface and one of the following conditions is true:

- The host mode differs from multi-host.
- MAC-Based or WEB-Based authentication is enabled.
- Radius VLAN assignment is enabled.

Examples

Example 1 - The following example puts the port `te1/0/`1 into Layer 2 mode.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# switchport
```

Example 2 - The following example puts the port `te1/0/`1 into Layer 3 mode.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# no switchport
```

59.11. switchport mode

Use thecommand `switchport mode` in Interface Configuration mode to configure the VLAN membership mode.

Use the `no` form of this command to restore the default configuration.

Syntax

- switchport mode {access|trunk|general|customer|vlan-mapping|private-vlan}
- no switchport mode

Parameters

- access - Specifies an untagged layer 2 VLAN port.
- trunk - Specifies a trunking layer 2 VLAN port.
- general - Specifies a full 802-1q-supported VLAN port.
- customer - Specifies that an edge port connected to customer equipment. Traffic received from this port will be tunneled with the additional 802.1q VLAN tag (Q-in-Q VLAN tunneling).
- vlan-mapping - vlan mapping modes
  - tunnel - vlan mapping tunnel mode
  - one-to-one - vlan mapping one-to-one mode
- private-vlan - private vlan modes
  - promiscuous - private-vlan promiscuous mode
  - host - private-vlan host port

Default Configuration

Access mode.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

When the port’s mode is changed, it receives the configuration corresponding to the mode.

If the port mode is changed to access and the access VLAN does not exist, then the port does not belong to any VLAN.

Note:
Preferred mode for RRP configuration is “general” as the one that supports all necessary VLAN management features.

The following features cannot be enabled if vlan-mapping is allowed:

- IPv4 routing
- Voice VLAN

The switchport vlan-mapping commands cannot add a port to a S-VLAN.

IPv4 and IPv6 interfaces cannot be defined on VLANs containing edge interfaces.

The following Layer 2 features are not supported into VLANs containing edge interfaces:

- IGMP Snooping
- MLD Snooping
- DHCP Snooping

Examples

Example 1 - The following example configures te1/0/1 as an access port (untagged layer 2) VLAN port.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# switchport mode access
switchxxxxxx(config-if)# switchport access vlan 2
```

Example 2 - The following example puts the port te1/0/2 into general mode.

```
switchxxxxxx(config)# interface te1/0/2
switchxxxxxx(config-if)# switchport mode general
```

59.12. switchport access vlan

A port in access mode can be an untagged member of at most a single VLAN. The switchport access vlan Interface Configuration command reassigns an interface to a different VLAN than it currently belongs or assigns it to none, in which case it is not a member of any VLAN.

The no form of this command to restore the default configuration.

Syntax

- switchport access vlan {vlan-id | none}
- no switchport access vlan

Parameters

- vlan-id - Specifies the VLAN to which the port is configured.
- none - Specifies that the access port cannot belong to any VLAN.

Default Configuration

The interface belongs to the Default VLAN.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

When the port is assigned to a different VLAN, it is automatically removed from its previous VLAN and added it to the new VLAN. If the port is assigned to none, it is removed from the previous VLAN and not assigned to any other VLAN.

A non-existed VLAN can be assigned as an Access VLAN. If the Access VLAN does not exist the `show interfaces switchport` command adds text "(Inactive)" after VLAN ID.

Example

The following example assigns access port te1/0/1 to VLAN 2 (and removes it from its previous VLAN).

```
switchxxxxxx(config)# interface te1/0/2
switchxxxxxx(config-if)# switchport mode access
switchxxxxxx(config-if)# switchport access vlan 2
```

59.13. switchport trunk allowed vlan

A trunk interface is an untagged member of a single VLAN, and, in addition, it may be an tagged member of one or more VLANs. Use the `switchport trunk allowed vlan` Interface Configuration mode command to add/remove VLAN(s) to/from a trunk port. Use the no form of the command to return to the default.

Syntax

- switchport trunk allowed vlan {all | none | add vlan-list | remove vlan-list | except vlan-list}
- no switchport trunk allowed vlan

Parameters

- all - Specifies all VLANs from 1 to 4094. At any time, the port belongs to all VLANs existing at the time. (range: 1–4094).
- none - Specifies an empty VLAN list The port does not belong to any VLAN.
- add vlan-list - List of VLAN IDs to add to the port. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- remove vlan-list - List of VLAN IDs to remove from a port. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- except vlan-list - List of VLAN IDs including all VLANs from range 1-4094 except VLANs belonging to vlan-list.

Default Configuration

By default, trunk ports belongs to all created VLANs.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use the switchport trunk allowed vlan command to specify which VLANs the port belongs to when its mode is configured as trunk.

Non-existed VLANs can be configured. When a non-existed VLAN is created the port will add to it automatically.

Forbidden VLANs can be configured.

Example

To add VLANs 2,3 and 100 to trunk ports 1 to 13

```
switchxxxxxx(config)# interface range te1/0/1-3
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport trunk allowed vlan add 2-3,100
switchxxxxxx(config-if)# exit
```

59.14. switchport trunk native vlan

If an untagged packet arrives on a trunk port, it is directed to the port's native VLAN. Use the `switchport trunk native vlan` Interface Configuration mode command to define the native VLAN for a trunk interface. Use the no form of this command to restore the default native VLAN.

Syntax

- switchport trunk native vlan {vlan-id | none}
- no switchport trunk native vlan

Parameters

- vlan-id - Specifies the native VLAN ID.
- none - Specifies the access port cannot belong to any VLAN.

Default Configuration

The default native VLAN is the Default VLAN.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

A value of the interface PVID is set to this VLAN ID.When the interface belongs to the Native VLAN it is set as VLAN untagged egress interface.

The configuration is applied only when the port mode is trunk.

Examples

The following example defines VLAN 2 as native VLAN for port `te1/0/1`:

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# switchport trunk native vlan 2
switchxxxxxx(config-if)# exit
```

59.15. switchport general allowed vlan

General ports can receive tagged or untagged packets.

Use the command `switchport general allowed vlan` in Interface Configuration mode to add/remove VLANs to/from a general port and configure whether packets on the egress are tagged or untagged.

Use the `no` form of this command to reset to the default.

Syntax

- switchport general allowed vlan add vlan-list [tagged|untagged]
- switchport general allowed vlan remove vlan-list
- no switchport general allowed vlan

Parameters

- add vlan-list - List of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs. (range: 1–4094)
- remove vlan-list - List of VLAN IDs to remove. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs (range: 1-4094).
- tagged - Specify that packets are transmitted tagged for the configured VLANs.
- untagged - Specify that packets are transmitted untagged for the configured VLANs (this is the default).

Default Configuration

The port is not a member of any VLAN.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

If the interface is a forbidden member of an added VLAN, the interface does not become a member of this specific VLAN. There will be an error message in this case ("An interface cannot become a a member of a forbidden VLAN. This message will only be displayed once.") and the command continues to execute in case if there are more VLANs in the vlan-list.

A non-existed VLAN cannot be configured. When a VLAN is removed it is deleted from the vlan-list.

Note:
The configuration is applied only when the port mode is general.

Example

The example adds te1/0/1 `and` to VLAN 2 and 3. Packets are tagged on the egress:

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# switchport general allowed vlan add 2-3 tagged
```

59.16. switchport general pvid

Use the `switchport general pvid` Interface Configuration mode command to configure the Port VLAN ID (PVID) of an interface when it is in general mode. Use the no form of this command to restore the default configuration.

Syntax

- switchport general pvid vlan-id
- no switchport general pvid

Parameters

- vlan-id - Specifies the Port VLAN ID (PVID).

Default Configuration

The PVID is the Default VLAN PVID.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Examples

Example 1 - The following example sets the te1/0/2 PVID to 234.

```
switchxxxxxx(config)# interface te1/0/2
switchxxxxxx(config-if)# switchport general pvid 234
```

Example 2 - The following example performs the following:

- Adds VLANs 2&3 as tagged, and VLAN 100 as untagged to te1/0/4
- Defines VID 100 as the PVID

```
switchxxxxxx(config)# interface te1/0/4
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general allowed vlan add 2-3 tagged
switchxxxxxx(config-if)# switchport general allowed vlan add 100 untagged
switchxxxxxx(config-if)# switchport general pvid 100
switchxxxxxx(config-if)# exit
```

59.17. switchport general ingress-filtering disable

Use the `switchport general ingress-filtering disable` Interface Configuration mode command to disable port ingress filtering (no packets are discarded at the ingress) on a general port. Use the no form of this command to restore the default configuration.

Syntax

- switchport general ingress-filtering disable
- no switchport general ingress-filtering disable

Parameters

N/A

Default Configuration

Ingress filtering is enabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example disables port ingress filtering on te1/0/1.

```
switchxxxxxx(config)# interface te1/0/1
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general ingress-filtering disable
```

59.18. switchport general acceptable-frame-type

The `switchport general acceptable-frame-type` Interface Configuration mode command configures the types of packets (tagged/untagged) that are filtered (discarded) on the interface. Use the no form of this command to return ingress filtering to the default.

Syntax

- switchport general acceptable-frame-type {tagged-only | untagged-only | all}
- no switchport general acceptable-frame-type

Parameters

- tagged-only - Ignore (discard) untagged packets and priority-tagged packets.
- untagged-only - Ignore (discard) VLAN-tagged packets (not including priority-tagged packets)
- all - Do not discard packets untagged or priority-tagged packets.

Default Configuration

All frame types are accepted at ingress (all).

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example configures port te1/0/3 to be in general mode and to discard untagged frames at ingress.

```
switchxxxxxx(config)# interface te1/0/3
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general acceptable-frame-type tagged-only
```

59.19. switchport general forbidden vlan

Use the `switchport general forbidden vlan` Interface Configuration mode command to forbid adding/removing specific VLANs to/from a port. Use the no form of this command to restore the default configuration.

Syntax

- switchport general forbidden vlan {add vlan-list | remove vlan-list}
- no switchport general forbidden vlan

Parameters

- add vlan-list - Specifies a list of VLAN IDs to add to interface. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- remove vlan-list - Specifies a list of VLAN IDs to remove from interface. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen designate a range of IDs.

Default Configuration

All VLANs are allowed.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The forbidden VLAN cannot be one that does not exist on the system, or one that is already defined on the port.

Example

The following example define s te1/0/4 as a forbidden membership in VLANs 5-7:

```
switchxxxxxx(config)# interface te1/0/4
switchxxxxxx(config-if)# switchport general forbidden vlan add 5-7
switchxxxxxx(config-if)# exit
```

59.20. switchport customer vlan

Use the `switchport customer vlan` Interface Configuration mode command to set the port's VLAN when the interface is in customer mode (set by the switchport mode command). Use the no form of this command to restore the default configuration.

Syntax

- switchport customer vlan vlan-id
- no switchport customer vlan

Parameters

- vlan-id - Specifies the customer VLAN.

Default Configuration

No VLAN is configured as customer.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

When a port is in customer mode it is in QinQ mode. This enables the user to use their own VLAN arrangements (PVID) across a provider network. The switch is in QinQ mode when it has one or more customer ports.

Example

The following example defines te1/0/4 as a member of customer VLAN 5.

```
switchxxxxxx(config)# interface te1/0/4
switchxxxxxx(config-if)# switchport mode customer
switchxxxxxx(config-if)# switchport customer vlan 5
```

59.21. switchport protected

Use the `switchport protected` Interface Configuration mode command to override the Filtering Database (FDB) decision, and send all Unicast, Multicast and Broadcast traffic to an uplink port. Use the no form of this command to disable overriding the FDB decision.

Syntax

- switchport protected interface-id
- no switchport protected

Parameters

- interface-id - Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.

Default Configuration

Switchport protected mode is disabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

This command overrides the FDB decision, and forwards packets to the uplink. Note that the packet is still subject to all filtering decisions.

A protected port cannot be a member of a VLAN with an IP interface.

Example

This example configures te1/0/2 s a protected port, so that all traffic is sent to its uplink (te1/0/3).

```
switchxxxxxx(config)# interface te1/0/2
switchxxxxxx(config-if)# switchport protected te1/0/3
```

59.22. map protocol protocols-group

Use the `map protocol protocols-group` VLAN Configuration mode command to map a protocol to a group of protocols. This protocol group can then be used in `switchport general map protocols-group vlan`. Use the no form of this command to delete a protocol from a group.

Syntax

- map protocol protocol [encapsulation-value] protocols-group group

- no map protocol protocol [encapsulation]

Parameters

- protocol - Specifies a 16-bit protocol number or one of the reserved names listed in the User Guidelines. (range: 0x0600–0xFFFF)
- encapsulation-value - Specifies one of the following values: Ethernet, rfc1042, llcOther.
- protocols-group group - Specifies the group number of the group of protocols (range: 1–2147483647).

Default Configuration

The default encapsulation value is Ethernet.

Command Mode

VLAN Database Configuration mode

User Guidelines

Forwarding of packets based on their protocol requires setting up groups of protocols and then mapping these groups to VLANs.

The value 0x8100 is not valid as the protocol number for Ethernet encapsulation.

The following protocol names are reserved for Ethernet Encapsulation:

- ip
- arp
- ipv6
- ipx

Example

The following example maps the IP protocol to protocol group number 213.

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# map protocol ip protocols-group 213
```

59.23. switchport general map protocols-group vlan

Use the `switchport general map protocols-group vlan` Interface Configuration mode command to forward packets based on their protocol, otherwise known as setting up a classifying rule. This command forwards packets arriving on an interface containing a specific protocol to a specific VLAN. Use the no form of this command to stop forwarding packets based on their protocol.

Syntax

- switchport general map protocols-group group vlan vlan-id
- no switchport general map protocols-group group

Parameters

- group - Specifies the group number as defined in map protocol protocols-group command (range: 1–65535).
- vlan-id - Defines the VLAN ID in the classifying rule.

Default Configuration

N/A

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The VLAN classification rule priorities are:

- MAC-based VLAN (best match among the rules)
- Subnet-based VLAN (best match among the rules)
- Protocol-based VLAN (up to 8 groups)
- PVID

Example

The following example forwards packets with protocols belong to protocol-group 1 to VLAN 8.

```
switchxxxxxx(config-if)# switchport general map protocols-group 1 vlan 8
```

59.24. show vlan protocols-groups

Use the `show vlan protocols-groups` EXEC mode command to display the protocols that belong to the defined protocols-groups.

Syntax

- show vlan protocols-groups

Parameters

N/A

Default Configuration

N/A

Command Mode

User EXEC mode

Example

The following example displays protocols-groups information.

```
switchxxxxxx# show vlan protocols-groups
Encapsulation Protocol Group ID
------------- -------- --------
Ethernet 0x800 (IP) 1
Ethernet 0x806 (ARP) 1
Ethernet 0x86dd (IPv6) 2
Ethernet 0x8898 3
```

59.25. map mac macs-group

Use the `map mac macs-group` VLAN Configuration mode command to map a MAC address or range of MAC addresses to a group of MAC addresses. Use the no form of this command to delete the mapping.

Syntax

- map mac macs-group mac-address {prefix-mask | host} group
- no map mac macs-group mac-address {prefix-mask | host}

Parameters

- mac-address - Specifies the MAC address to be mapped to the group of MAC addresses.
- prefix-mask - Specifies the number of ones in the mask.
- host - Specifies that the mask is comprised of all 1s.
- group - Specifies the group number (range: 1–2147483647)

Default Configuration

N/A

Command Mode

VLAN Database Configuration mode

User Guidelines

Forwarding of packets based on their MAC address requires setting up groups of MAC addresses and then mapping these groups to VLANs.

Up to 256 MAC addresses (host or range) can be mapped to one or many MAC-based VLAN groups.

Example

The following example creates two groups of MAC addresses, sets a port to general mode and maps the groups of MAC addresses to specific VLANs.

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# map mac 0000.1111.0000 32 macs-group 1
switchxxxxxx(config-vlan)# map mac 0000.0000.2222 host macs-group 2
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)# interface te1/0/4
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general map macs-group 1 vlan 2
switchxxxxxx(config-if)# switchport general map macs-group 2 vlan 3
```

59.26. switchport general map macs-group vlan

Use the `switchport general map macs-group vlan` Interface Configuration mode command to set a MAC-based classification rule. Use the no form of this command to delete a classification rule.

Syntax

- switchport general map macs-group group vlan vlan-id
- no switchport general map macs-group group

Parameters

- group - Specifies the group number (range: 1–2147483647)
- vlan-id - Defines the VLAN ID associated with the rule.

Default Configuration

N/A

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

MAC-based VLAN rules cannot contain overlapping ranges on the same interface.

The VLAN classification rule priorities are:

- MAC-based VLAN (best match among the rules)
- Subnet-based VLAN (best match among the rules)
- Protocol-based VLAN
- PVID

User Guidelines

After groups of MAC addresses have been created (see the `map mac macs-group` command), they can be mapped to specific VLANs.

Each MAC address (host or range) in the MAC-based group assigned to an interface consumes a single TCAM entry.

Example

The following example creates two groups of MAC addresses, sets a port to general mode and maps the groups of MAC addresses to specific VLANs.

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# map mac 0000.1111.0000 32 macs-group 1
switchxxxxxx(config-vlan)# map mac 0000.0000.2222 host macs-group 2
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)# interface te1/0/4
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general map macs-group 1 vlan 2
switchxxxxxx(config-if)# switchport general map macs-group 2 vlan 3
```

59.27. show vlan macs-groups

Use the `show vlan macs-groups` EXEC mode command to display the MAC addresses that belong to the defined MAC-based classification rules.

Syntax

- show vlan macs-groups

Parameters

N/A

Default Configuration

N/A

Command Mode

User EXEC mode

Example

The following example displays defined MAC-based classification rules.

```
switchxxxxxx# show vlan macs-groups
 MAC Address Mask Group ID
-------------------- -------------------- --------------------
 00:12:34:56:78:90 20 22
 00:60:70:4c:73:ff 40 1
```

59.28. map subnet subnets-group

Use the `map subnet subnets-group` VLAN Configuration mode command to map an IP subnet to a group of IP subnets. Use the no form of this command to delete the map.

Syntax

- map subnet subnets-group ip-address prefix-mask group
- no map subnet ip-address prefix-mask

Parameters

- ip-address - Specifies the IP address prefix of the subnet to be mapped to the group.
- prefix-mask - Specifies the number of 1s in the mask.
- group - Specifies the group number. (range: 1–2147483647)

Default Configuration

N/A

Command Mode

VLAN Database Configuration mode

User Guidelines

Forwarding of packets based on their IP subnet requires setting up groups of IP subnets and then mapping these groups to VLANs.

Example

The following example maps an IP subnet to the group of IP subnets 4. It then maps this group of IP subnets to VLAN 8

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# map subnet 172.16.1.1 24 subnets-group 4
switchxxxxxx(config-vlan)# switchport general map subnets-group 4 vlan 8
```

59.29. switchport general map subnets-group vlan

Use the `switchport general map subnets-group vlan` Interface Configuration mode command to set a subnet-based classification rule. Use the no form of this command to delete a subnet-based classification rule.

Syntax

- switchport general map subnets-group group vlan vlan-id
- no switchport general map subnets-group group

Parameters

- group - Specifies the group number. (range: 1–2147483647)
- vlan-id - Defines the VLAN ID associated with the rule.

Default Configuration

N/A

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The VLAN classification rule priorities are:

- MAC-based VLAN (Best match among the rules)
- Subnet-based VLAN (Best match among the rules)
- Protocol-based VLAN
- PVID

Example

The following example maps an IP subnet to the group of IP subnets 4. It then maps this group of IP subnets to VLAN 8

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# map subnet 172.16.1.1 24 subnets-group 4
switchxxxxxx(config-vlan)# switchport general map subnets-group 4 vlan 8
```

59.30. show vlan subnets-groups

Use the `show vlan subnets-groups` EXEC mode command to display subnets-groups information.

Syntax

- show vlan subnets-groups

Parameters

N/A

Default Configuration

N/A

Command Mode

User EXEC mode

Example

The following example displays subnets-groups information.

```
switchxxxxxx# show vlan subnets-groups
IP Subnet Address Mask Group ID
----------------- ----------- --------------
 1.1.1.1 32 1
 172.16.2.0 24 2
```

59.31. show interfaces switchport

Use the `show interfaces switchport` Privileged EXEC command to display the administrative and operational status of all interfaces or a specific interface.

Syntax

- show interfaces switchport [interface-id]

Parameters

- Interface-id - Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.

Command Mode

Privileged EXEC mode

Default

Displays the status of all interfaces.

User Guidelines

Each port mode has its own private configuration. The show interfaces switchport command displays all these configurations, but only the port mode configuration that corresponds to the current port mode displayed in "Administrative Mode" is active.

Example

```
switchxxxxxx# show interfaces switchport te1/0/1
Gathering information...
Name: te1/0/1
Switchport: enable
Administrative Mode: access
Operational Mode: down
Access Mode VLAN: 1
Access Multicast TV VLAN: none
Trunking Native Mode VLAN: 1
Trunking VLANs: 1
 2-4094 (Inactive)
General PVID: 1
General VLANs: none
General Egress Tagged VLANs: none
General Forbidden VLANs: none
General Ingress Filtering: enabled
General Acceptable Frame Type: all
General GVRP status: Enabled
General GVRP VLANs: none
Customer Mode VLAN: none
Private-vlan promiscuous-association primary VLAN: none
Private-vlan promiscuous-association Secondary VLANs: none
Private-vlan host-association primary VLAN: none
Private-vlan host-association Secondary VLAN: none
Protected: Enabled, Uplink is te1/0/1 Classification rules:
Classification Type Group ID VLAN ID
------------------- -------- -------
Protocol 1 19
Protocol 1 20
Protocol 2 72
Subnet 1 15
MAC 1 77
```

59.32. private-vlan

Use the `private-vlan` Interface VLAN Configuration mode command to configure a private VLAN. Use the no form of this command to return the VLAN to normal VLAN configuration.

Syntax

- private-vlan {primary | community | isolated}
- no private-vlan

Parameters

- primary - Designate the VLAN as a primary VLAN.
- community - Designate the VLAN as a community VLAN.

- isolated - Designate the VLAN as an isolated VLAN.

Default Configuration

No private VLANs are configured.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

- The VLAN type cannot be changed if there is a private VLAN port that is a member in the VLAN.
- The VLAN type cannot be changed if it is associated with other private VLANs. The VLAN type is not kept as a property of the VLAN when the VLAN is deleted.

Example

The following example set vlan 2 to be primary vlan:

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# private-vlan primary
```

59.33. private-vlan association

Use the `private-vlan association` Interface VLAN Configuration mode command to configure the association between the primary VLAN and secondary VLANs. Use the no form of this command to remove the association.

Syntax

- private-vlan association [add | remove] secondary-vlan-list
- no private-vlan association

Parameters

- add secondary-vlan-list - List of VLAN IDs of type secondary to add to a primary VLAN. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.This is the default action.
- remove secondary-vlan-list - List of VLAN IDs of type secondary to remove association from a primary VLAN. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.

Default Configuration

No private VLANs are configured.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

- The command can only be executed in the context of the primary VLAN.
- A private VLAN cannot be removed or have its type changed, if it is associated with other private VLANs.
- A primary VLAN can be associated with only a single, isolated VLAN.
- A secondary VLAN can be associated with only one primary VLAN.
- The association of secondary VLANs with a primary VLAN cannot be removed if there are private VLAN ports that are members in the secondary VLAN.

- In MSTP mode, all the VLANs that are associated with a private VLAN must be mapped to the same instance.

Example

The following example associate secondary VLAN 20,21,22 and 24 to primary VLAN 2.

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# private-vlan association add 20-22,24
```

59.34. switchport private-vlan mapping

Use the `switchport private-vlan mapping` Interface Configuration mode command to configure the VLANs of the private VLAN promiscuous port. Use the no form of this command to reset to default.

Syntax

- switchport private-vlan mapping primary-vlan-id [add | remove] secondary-vlan-list
- no switchport private-vlan mapping

Parameters

- primary-vlan-id - The VLAN ID of the primary VLAN.
- add secondary-vlan-list - Specifies one or more secondary VLANs to be added to the port.
- remove secondary-vlan-list - Specifies one or more secondary VLANs to be removed from the port.

Default Configuration

No VLAN is configured.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The secondary VLANs should be associated with the primary VLANs, otherwise the configuration is not accepted.

Example

The following example add promiscuous port te1/0/4 to primary VLAN 10 and to secondary VLAN 20.

```
switchxxxxxx(config)# interface te1/0/4
switchxxxxxx(config-if)# switchport private-vlan mapping 10 add 20
```

59.35. switchport private-vlan host-association

Use the `switchport private-vlan host-association` Interface Configuration mode command to configure the association of a host port with primary and secondary VLANs of the private VLAN. Use the no form of this command to reset to default.

Syntax

- switchport private-vlan host-association primary-vlan-id secondary-vlan-id
- no switchport private-vlan host-association

Parameters

- primary-vlan-id - The VLAN ID of the primary VLAN. secondary-vlan-id - Specifies the secondary VLAN.

Default Configuration

No association.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The secondary VLAN must be associated with the primary VLAN, otherwise the configuration is not accepted. See the private-vlan association command.

The port association configuration depends on the type of the secondary VLAN.

- The port association configuration for a community secondary VLAN includes: The port is added as untagged to the primary VLAN and to the secondary VLAN.
- The PVID is set to the VLAN-ID of the secondary VLAN.
- The port ingress filtering is enabled.
- The port association configuration for an isolated secondary VLAN includes: The port is added as untagged only to the primary VLAN and is not added to the secondary VLAN.
- The PVID is set to the VLAN-ID of the secondary VLAN.
- The port ingress filtering is disabled.

Example

The following example set port te1/0/4 to secondary VLAN 20 in primary VLAN 10.

```
switchxxxxxx(config)# interface te1/0/4
switchxxxxxx(config-if)# switchport private-vlan host-association 10 20
```

59.36. show vlan private-vlan

Use the `show vlan private-vlan` EXEC mode command to display private VLAN information.

Syntax

- show vlan private-vlan [tag vlan-id]

Parameters

- tag vlan-id - Primary VLAN that represent the private VLAN to be displayed.

Default Configuration

All private VLANs are displayed.

Command Mode

User EXEC mode

User Guidelines

The show vlan private-vlan command does not include non-private VLAN ports that are members in private VLANs. Tag parameters of non-primary VLAN will result in an empty show output.

Example

```
switchxxxxxx# show vlan private-vlan
 Primary Secondary Type Ports
---------- ---------- ---------- ----------------------
 150 primary te1/0/1
 150 151 isolated te1/0/2
 160 primary te1/0/3 160 161 community te1/0/4
switchxxxxxx# show vlan private-vlan 150
 Primary Secondary Type Ports
---------- ---------- ---------- ----------------------
 150 primary te1/0/1
 150 151 isolated te1/0/4
```

59.37. switchport access multicast-tv vlan

To assign a Multicast-TV VLAN to an access port, use the `switchport access multicast-tv vlan` command in Interface (Ethernet, Port Channel) Configuration mode. To return to the default, use the no format of the command.

Syntax

- switchport access multicast-tv vlan vlan-id
- no switchport access multicast-tv vlan

Parameters

- vlan-id - Specifies the Multicast TV VLAN ID.

Default Configuration

Receiving Multicast transmissions is disabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

When the port is assigned to a different Multicast-TV VLAN, it is automatically removed from its previous VLAN and added it to the new Multicast-TV VLAN.

When an existed Multicast-TV VLAN is assigned to an access port, the multicast messages received on a membership of the Multicast-TV VLAN are forwarded to the access port. All messages received on the access port are bridged only into its Access VLAN.

To register IGMP reports arriving on the access port by IGMP Snooping running on the Multicast-TV VLAN, use the `ip igmp snooping map cpe vlan` command.

A non-existed VLAN can be assigned as a Multicast-TV VLAN. If the Multicast-TV VLAN does not exist the `show interfaces switchport` command adds text "(Inactive)" after VLAN ID.

Example

The following example enables te1/0/4 to receive Multicast transmissions from VLAN 11.

```
switchxxxxxx(config)# interface te1/0/4
switchxxxxxx(config-if)# switchport access multicast-tv vlan 11
```

59.38. switchport customer multicast-tv vlan

To assign Multicast-TV VLANs to a customer port, use the `switchport customer multicast-tv vlan` command in Interface (Ethernet, Port Channel) Configuration mode. To return to the default, use the no format of the command.

Syntax

- switchport customer multicast-tv vlan {add vlan-list | remove vlan-list}

Parameters

- add vlan-list - Specifies a list of Multicast TV VLANs to add to interface.
- remove vlan-list - Specifies a list of Multicast TV VLANs to remove from interface.

Default Configuration

The port is not a member in any Multicast TV VLAN.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

When an existed Multicast-TV VLAN is assigned to a customer port, the multicast messages received on a membership of the Multicast-TV VLAN are forwarded to the customer port. All messages received on the customer port are not bridged only into the Multicast-TV VLAN.

To register IGMP reports arriving on the customer port by IGMP Snooping running on the Multicast-TV VLAN, use the `ip igmp snooping map cpe vlan` command.

A non-existed VLAN can be assigned as a Multicast-TV VLAN. If the Multicast-TV VLAN does not exist the `show interfaces switchport` command adds text "(Inactive)" after VLAN ID.

Example

The following example enables te1/0/4 to receive Multicast transmissions from VLANs 5, 6, 7.

```
switchxxxxxx(config)# interface te1/0/4
switchxxxxxx(config-if)# switchport customer multicast-tv vlan add 5-7
```

59.39. show vlan multicast-tv

Use the `show vlan Multicast-tv` EXEC mode command to display the source and receiver ports of Multicast-TV VLAN. Source ports can transmit and receive traffic to/from the VLAN, while receiver ports can only receive traffic from the VLAN.

Syntax

- show vlan Multicast-tv vlan vlan-id

Parameters

- vlan-id - Specifies the VLAN ID.

Default Configuration

N/A

Command Mode

User EXEC mode

Example

The following example displays information on the source and receiver ports of Multicast-TV VLAN 1000.

```
switchxxxxxx# show vlan multicast-tv vlan 1000
Source Ports Receiver Ports
------------ --------------------
te1/0/3, te1/0/4 te1/0/1-2
```

59.40. vlan prohibit-internal-usage

Use the `vlan prohibit-internal-usage` command in Global configuration mode to specify VLANs that cannot be used by the switch as internal VLANs.

Syntax

- vlan prohibit-internal-usage none | {add | except | remove} vlan-list

Parameters

- none - The Prohibit Internal Usage VLAN list is empty: any VLAN can be used by the switch as internal.
- except - The Prohibit Internal Usage VLAN list includes all VLANs except the VLANs specified by the vlan-list argument: only the VLANs specified by the vlan-list argument can be used by the switch as internal.
- add - Add the given VLANs to the Prohibit Internal Usage VLAN list.
- remove - Remove the given VLANs from the Prohibit Internal Usage VLAN list.
- vlan-list - List of VLAN. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs. The VLAN ID that can be used is from 1 through 4094.

Default Configuration

The Prohibit Internal usage VLAN list is empty.

Command Mode

Global Configuration mode

User Guidelines

The switch requires an internal VLAN in the following cases:

- One VLAN for each IP interface is defined directly on an Ethernet port or on a Port channel.
- One VLAN for each IPv6 tunnel.
- One VLAN for 802.1x.

When a switch needs an internal VLAN it takes a free VLAN with the highest VLAN ID.

Use the vlan prohibit-internal-usage command to define a list of VLANs that cannot be used as internal VLANs after reload.

If a VLAN was chosen by the software for internal usage, but you want to use that VLAN for a static or dynamic VLAN, do one of the following

- Add the VLAN to the Prohibited User Reserved VLAN list.
- Copy the Running Configuration file to the Startup Configuration file
- Reload the switch
- Create the VLAN

Examples

Example 1 - The following example specifies that VLANs 4010, 4012, and 4090-4094 cannot be used as internal VLANs:

```
vlan prohibit-internal-usage add 4010,4012,4090-4094
```

Example 2 - The following specifies that all VLANs except 4000-4107 cannot be used as internal VLANs:

```
vlan prohibit-internal-usage all vlan prohibit-internal-usage remove 4000-4107
```

Example 3 - The following specifies that all VLANs except 4000-4107 cannot be used as internal VLANs:

```
vlan prohibit-internal-usage 4000-4107
```

59.41. show vlan internal usage

Use the `show vlan internal usage` Privileged EXEC mode command to display a list of VLANs used internally by the device (defined by the user).

Syntax

- show vlan internal usage

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays VLANs used internally by the switch:

```
show vlan internal usage
User Reserved VLAN list after reset: 4010,4012,4080-4094
Current User Reserved VLAN list: 4010,4012,4090-4094
VLAN Usage
---- --------
4089 te1/0/2
4088 te1/0/3
4087 tunnel 1
4086 802.1x
```

60. Voice VLAN Commands

60.1. show voice vlan

To display the voice VLAN status for all interfaces or for a specific interface if the voice VLAN type is OUI, use the `show voice vlan` Privileged EXEC mode command.

Syntax

- show voice vlan [type oui [{interface-id | detailed}]]

Parameters

- type oui - (Optional) Common and OUI-voice-VLAN specific parameters are displayed.
- interface-id - (Optional) Specifies an Ethernet port ID.
- detailed - (Optional) Displays information for non-present ports in addition to present ports.

Default Configuration

If the type parameter is omitted the current Voice VLAN type is used.

If the interface-id parameter is omitted then information about all present interfaces is displayed. If detailed is used, non-present ports are also displayed.

Command Mode

Privileged EXEC mode

User Guidelines

Using this command without parameters displays the current voice VLAN type parameters and local and agreed voice VLAN settings.

Using this command with the type parameter displays the voice VLAN parameters relevant to the type selected. The the local and agreed voice VLAN settings are displayed only if this is the current voice VLAN state.

The interface-id parameter is relevant only for the OUI VLAN type.

Examples

The following example displays the voice VLAN parameters.

```
switch>show voice vlan
Administrate Voice VLAN state is oui-enabled
The Operational Voice VLAN-ID is 2
Aging timeout: 1440 minutes
CoS: 6
Remark: Yes
OUI table
MAC Address - Prefix Description
------------------- ------------------
00:E0:BB 3COM
00:03:6B Cisco
00:E0:75 Veritel
00:D0:1E Pingtel
00:01:E3 Simens
00:60:B9 NEC/Philips
00:0F:E2 Huawei-3COM
00:09:6E Avaya
```

```
Interface Enabled Secure Activated CoS Mode
------------ ------- ------- --------- -------
te1/0/1 Yes Yes Yes all
te1/0/2 Yes Yes No src
te1/0/3 No No
```

60.2. voice vlan state

To set the type of voice VLAN that is functional on the device or disable voice VLAN entirely, use the `voice vlan state` Global Configuration mode command.

The no format of the command returns to the default.

Syntax

- voice vlan state {oui-enabled | disabled]
- no voice vlan state

Parameters

- oui-enabled - Voice VLAN is of type OUI.
- disabled - Voice VLAN is disabled.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

If the administrative state is:

- disabled - The operational state is disabled.
- oui-enabled - The operational state is oui-enabled.

Examples

Example 1 - The following example enables the OUI mode of Voice VLAN. The first try did not work - it was necessary to first disable voice VLAN.

```
switchxxxxxx(config)# voice vlan state oui-enabled Disable the voice VLAN before
changing the voice VLAN trigger.
switchxxxxxx(config)# voice vlan state disabled
switchxxxxxx(config)# voice vlan state oui-enabled
```

60.3. voice vlan id

To statically configure the VLAN identifier of the voice VLAN, use the `voice vlan id` Global Configuration mode command. To return the voice VLAN to the default VLAN (1), use the no format of the command.

Syntax

- voice vlan id vlan-id
- no voice vlan id

Parameters

- vlan id vlan-id - Specifies the voice VLAN (range 1-4094).

Default Configuration

VLAN ID 1.

Command Mode

Global Configuration mode

User Guidelines

If the Voice VLAN does not exist, it is created automatically. It will not be removed automatically by the no version of this command.

Example

The following example enables VLAN 35 as the voice VLAN on the device.

```
switchxxxxxx(config)# voice vlan id 35
For Auto Voice VLAN, changes in the voice VLAN ID, CoS/802.1p, and/or DSCP will
cause the switch to advertise the administrative voice VLAN as static voice VLAN
which has higher priority than voice VLAN learnt from external sources.
Are you sure you want to continue? (Y/N)[Y] Y
30-Apr-2011 00:19:36 %VLAN-I-VoiceVlanCreated: Voice Vlan ID 35 was created.
switchxxxxxx(config)# 30-Apr-2011 00:19:51 %VLAN-I-ReceivedFromVSDP: Voice VLAN
updated by VSDP. Voice VLAN-ID 35, VPT 5, DSCP 46
```

60.4. voice vlan oui-table

To configure the voice OUI table, use the `voice vlan oui-table` Global Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- voice vlan oui-table {add mac-address-prefix | remove mac-address-prefix} [text]
- no voice vlan oui-table

Parameters

- add mac-address-prefix - Adds the specified MAC address prefix to the voice VLAN OUI table (length: 3 bytes).
- remove mac-address-prefix - Removes the specified MAC prefix address from the voice VLAN OUI table (length: 3 bytes).
- text - (Optional) Adds the specified text as a description of the specified MAC address to the voice VLAN OUI table (length: 1–32 characters).

Default Configuration

The default voice VLAN OUI table is:

OUI	Description
00:01:e3	Siemens AG Phone
00:03:6b	Cisco Phone
00:09:6e	Avaya Phone
00:0f:e2	Huawei-3COM Phone
00:60:b9	NEC/Philips Phone
00:d0:1e	Pingtel Phone

00:e0:75	Veritel Polycom Phone
00:e0:bb	3COM Phone

Command Mode

Global Configuration mode

User Guidelines

The classification of a packet from VoIP equipment/phones is based on the packet's OUI in the source MAC address. OUIs are globally assigned (administered) by the IEEE.

In MAC addresses, the first three bytes contain a manufacturer ID

(Organizationally Unique Identifiers (OUI)) and the last three bytes contain a unique station ID.

Since the number of IP phone manufacturers that dominates the market is limited and well known, the known OUI values are configured by default and OUIs can be added/removed by the user when required.

Example

The following example adds an entry to the voice VLAN OUI table.

```
switchxxxxxx(config)# voice vlan oui-table add 00:AA:BB experimental
```

60.5. voice vlan cos mode

To select the OUI voice VLAN Class of Service (CoS) mode, use the `voice vlan cos mode` Interface Configuration mode command. To return to the default, use the no form of this command.

Syntax

- voice vlan cos mode {src | all }
- no voice vlan cos mode

Parameters

- src - QoS attributes are applied to packets with OUIs in the source MAC address. See the User Guidelines of `voice vlan oui-table`.
- all - QoS attributes are applied to packets that are classified to the Voice VLAN.

Default Configuration

The default mode is src.

Command Mode

Interface Configuration mode

Example

The following example applies QoS attributes to voice packets.

```
switchxxxxxx(config-if)# voice vlan cos mode all
```

60.6. voice vlan cos

To set the OUI Voice VLAN Class of Service (CoS), use the `voice vlan cos` Global Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- voice vlan cos cos [remark]
- no voice vlan cos

Parameters

- cos cos - Specifies the voice VLAN Class of Service value. (Range: 0–7)
- remark - (Optional) Specifies that the L2 user priority is remarked with the CoS value.

Default Configuration

The default CoS value is 5.

The L2 user priority is not remarked by default.

Command Mode

Global Configuration mode

Example

The following example sets the OUI voice VLAN CoS to 7 and does not do remarking.

```
switchxxxxxx(config)# voice vlan cos 7
```

60.7. voice vlan aging-timeout

To set the OUI Voice VLAN aging timeout interval, use the `voice vlan aging-timeout` Global Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- voice vlan aging-timeout minutes
- no voice vlan aging-timeout

Parameters

aging-timeout minutes - Specifies the voice VLAN aging timeout interval in minutes. (Range: 1–43200).

Default Configuration

1440 minutes

Command Mode

Global Configuration mode

Example

The following example sets the OUI Voice VLAN aging timeout interval to 12 hours.

```
switchxxxxxx(config)# voice vlan aging-timeout 720
```

60.8. voice vlan enable

To enable OUI voice VLAN configuration on an interface, use the `voice vlan enable` Interface Configuration mode mode command. To disable OUI voice VLAN configuration on an interface, use the no form of this command.

Syntax

- voice vlan enable

- no voice vlan enable

Parameters

This command has no arguments or keywords.

Default Configuration

Disabled

Command Mode

Interface Configuration mode

User Guidelines

This command is applicable only if the voice VLAN state is globally configured as OUI voice VLAN (using `show voice vlan`).

The port is added to the voice VLAN if a packet with a source MAC address OUI address (defined by `voice vlan oui-table`) is trapped on the port. Note: The packet VLAN ID does not have to be the voice VLAN, it can be any VLAN.

The port joins the voice VLAN as a tagged port.

If the time since the last MAC address with a source MAC address OUI address was received on the interface exceeds the timeout limit (configured by `voice vlan aging-timeout`), the interface is removed from the voice VLAN.

Example

The following example enables OUI voice VLAN configuration on `te1/0/2`.

```
switchxxxxxx(config)# interface te1/0/2
switchxxxxxx(config-if)# voice vlan enable
```

61. VRRP Commands

61.1. clear vrrp counters

To clear the VRRP counters, use the `clear vrrp counters` command in Privileged EXEC mode.

Syntax

- clear vrrp counters [interface-id]

Parameters

- interface-id - (Optional) Interface Identifier.

Default Configuration

No description.

Command Mode

Privileged EXEC mode

User Guidelines

Use this command without the identifier-id argument to clear the VRRP counters of all interfaces where Virtual routers are running.

Use this command with the identifier-id argument to clear the VRRP counters of the specified interface.

Example

The following example shows how to clear the counters of all VRRP virtual routers running on VLAN 10:

```
switchxxxxxx# clear vrrp counters vlan10
```

61.2. show vrrp

To display a brief or detailed status of one or all configured VRRP virtual routers, use the `show vrrp` command in Privileged EXEC mode.

Syntax

- show vrrp [all | brief | interface interface-id]

Parameters

- all - (Optional) Provides VRRP virtual router information about all VRRP virtual routers, including virtual routers in disable status. If no keyword is configured, the all keyword is applied.
- brief - (Optional) Provides a summary view of the VRRP virtual router information
- interface interface-id - (Optional) Interface identifier

Command Mode

Privileged EXEC mode

User Guidelines

Use this command with the all keyword or without keywords to display the VRRP status of all configured VRRP virtual routers.

Use this command with the identifier-id argument to clear the VRRP counters of the specified interface.

Examples

Example 1. The following example displays a detailed VRRP status of all configured VRRP virtual routers:

```
switchxxxxxx# show vrrp
Interface: VLAN 10
Virtual Router 1
Virtual Router name CLUSTER1
Supported version is VRRPv3
State is Master
Virtual IP addresses are 10.2.0.10, 10.3.0.10(down)
Source IP address is 10.3.0.20 is down; a default Source IP address of 10.2.0.10
is applied
Virtual MAC address is 00:00:5e:00:01:01
Advertisement interval is 3.000 sec
Preemption enabled
Priority is 100
Master Router is 10.3.0.20 (local), priority is 100
Master Advertisement interval is 3.000 sec
Master Down Interval is 10.828 sec
Interface: VLAN 10
Virtual Router 2
Supported version is VRRPv3
State is Master
Virtual Router name CLUSTER2
Virtual IP addresses are 10.4.0.20, 10.5.0.20
Source IP address is 10.4.0.20(default)
Virtual MAC address is 00:00:5e:00:01:02
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 255
Master Router is 10.4.0.20 (local), priority is 255
Master Advertisement interval is 1.000 sec
Master Down Interval is 3.629 sec
Skew Time is 1.000 sec
Interface: VLAN 50 Virtual Router 1
Supported version is VRRPv3
State is Backup
Virtual Router name CLUSTER3
Virtual IP addresses are 10.6.0.10
Source IP address is 10.6.0.20(default)
Virtual MAC address is 00:00:5e:00:01:01 Advertisement interval is 1.000 sec
Preemption enabled
Priority is 95
Master Router is 10.6.0.10, priority is 255
Master Advertisement interval is 1.000 sec
Master Down Interval is 3.629 sec
Skew Time is 0.628 sec
Interface VLAN 400
Virtual Router 4
Supported version is VRRPv3
State is Initializing
Virtual Router name CLUSTER4
```

```
Virtual IP addresses are 10.7.0.10
Source IP address is 10.7.0.20
Virtual MAC address is 00:00:5e:00:01:03
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 150
```

Example 2. The following example displays a detailed VRRP status of VRRP virtual routers running on VLAN 10:

```
switchxxxxxx# show vrrp interface vlan10
Interface: VLAN 10
Virtual Router 1
Virtual Router name CLUSTER1
Supported version is VRRPv3
State is Master
Virtual IP addresses are 10.2.0.10, 10.3.0.10
Source IP address is 10.3.0.20
Virtual MAC address is 00:00:5e:00:01:01
Advertisement interval is 3.000 sec
Preemption enabled
Priority is 100
Master Router is 10.3.0.10 (local), priority is 100
Master Advertisement interval is 3.000 sec
Master Down Interval is 10.828 sec
Interface: VLAN 10
Virtual Router 2
Supported version is VRRPv3
State is Master
Virtual Router name CLUSTER2
Virtual IP addresses are 10.4.0.10, 10.5.0.10
Source IP address is 10.4.0.10
Virtual MAC address is 00:00:5e:00:01:02
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 95
Master Router is 10.4.0.10 (local), priority is 95
Master Advertisement interval is 1.000 sec
Master Down Interval is 3.629 sec
```

Example 3. The following example displays a brief VRRP status of all configured VRRP virtual routers:

```
switchxxxxxx# show vrrp brief
State (S): I - Initialize; M - Master; B - Backup
Preempt (P): Y - Yes; N - No
Interface VR Virtual Pri Timer P St Ver Source address Master
 Address Address Address
--------- --- -------------- --- ----- - -- --- --------------- ----------------
-
VLAN 10 1 10.2.0.10 100 3000 Y M 3 10.3.0.10 10.3.0.10 10.3.0.10
VLAN 10 2 10.4.0.10 255 1000 Y M 3 10.4.0.10 10.4.0.10
 10.5.0.10
VLAN 50 1 10.6.0.10 95 1000 Y B 3 10.6.0.10 10.6.0.60
VLAN 400 4 10.7.0.20 150 1000 Y I 3 10.7.0.10
```

61.3. show vrrp counters

To display the VRRP counters, use the `show vrrp counters` command in Privileged EXEC mode.

Syntax

- show vrrp counters [interface-id]

Parameters

- interface-id - (Optional) Interface Identifier.

Command Mode

Privileged EXEC mode

User Guidelines

Use the show vrrp counters command without the identifier-id argument to display the VRRP counters of all interfaces where Virtual routers are running.

Use the show vrrp counters command with the identifier-id argument to display the VRRP counters of the specified interface.

Example

The following example display the counters of all virtual routers defined on VLAN 100:

```
switchxxxxxx# show vrrp counters vlan 100 vlan 100
 Invalid checksum: 0
 Invalid Packet Length: 0
 Invalid TTL: 0
 Invalid VRRP Packet Type: 0
 Invalid VRRP ID: 0
 Invalid Protocol Number: 0
 Invalid IP List: 0
 Invalid Interval: 0
 Invalid Authentication: 0
```

61.4. vrrp description

To assign a description to the VRRP virtual router, use the `vrrp description` command in Interface Configuration mode. To return to the default, use the no format of the command.

Syntax

- vrrp vrid description text
- no vrrp vrid description

Parameters

- vrid - Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.
- text - Text that describes the purpose or use of the virtual router. The parameter may contain 0-160 characters.

Default Configuration

No description.

Command Mode

Interface Configuration mode

Example

The following example shows how to assign a VRRP description to the specified VRRP virtual router:

```
switchxxxxxx(config)# interface vlan 10
switchxxxxxx(config-if)# vrrp 1 description router1
switchxxxxxx(config-if)# exit
```

61.5. vrrp ip

To define an IP address of a virtual router, use the `vrrp ip` command in Interface Configuration mode. To remove the IP address, use the no format of the command.

Syntax

- vrrp vrid ip ip-address
- no vrrp vrid ip [ip-address]

Parameters

- vrid - Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.
- ip-address - Virtual router's IP address.

Command Mode

Interface Configuration mode

User Guidelines

A virtual router comes into existence when it has one or more participating VRRP routers. To participate in a specific virtual router as a VRRP router, use vrrp ip to configure an existing IP interface with the identifier and the IP address(es) of the virtual router. The IP interface of the VRRP router and the virtual router must be in the same IP subnet.

A VRRP router that is the owner if the virtual router's IP address(es) is also the VRRP router real IP address at the IP interface. There is only one owner for all virtual router's IP address(es). A VRRP router participates in a virtual router when it is configured with the first virtual router's IP address and does not participate when the virtual router IP address is removed.

A virtual router entity in a VRRP router is created in the shutdown state. Use the no vrrp shutdown command to enable it.

To defined more than one virtual router's IP address, the command should be applied for each configured IP address.

Each VRRP router in the virtual router should be configured with the same set of IP addresses.

If the ip-address parameter is omitted in the no format of the CLI command, all the IP addresses of the virtual router are removed, leading to the virtual router entity in the VRRP router being removed too.

The switch supports up to 255 VRRP routers.

Example

The following example shows how to define a VRRP virtual router:

```
switchxxxxxx(config)# interface vlan 10
switchxxxxxx(config-if)# vrrp 1 ip 192.168.2.1
switchxxxxxx(config-if)# exit
```

61.6. vrrp preempt

To enable Virtual Router Redundancy Protocol (VRRP) preemption, use the `vrrp preempt` command in Interface Configuration mode. To return to the default, use the no format of the command.

Syntax

- vrrp vrid preempt
- no vrrp vrid preempt

Parameters

- vrid - Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.

Command Mode

Interface Configuration mode

Default Configuration

Preemption is enabled by default.

User Guidelines

By default, the VRRP router being configured with this command will take over as Master virtual router for the group if it has a higher priority than the current master virtual router.

Note: The router that is the IP address owner will preempt, regardless of the setting of this command.

Example

The following example shows how to disable VRRP preemption to the specified VRRP virtual router:

```
switchxxxxxx(config)# interface vlan 10
switchxxxxxx(config-if)# no vrrp 1 preempt
switchxxxxxx(config-if)# exit
```

61.7. vrrp priority

To define Virtual Router Redundancy Protocol (VRRP) priority, use the `vrrp priority` command in Interface Configuration mode. To return to the default, use the no format of the command.

Syntax

- vrrp vrid priority priority
- no vrrp vrid priority

Parameters

- vrid - Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.
- priority - Virtual router priority. The range is 1-254.

Command Mode

Interface Configuration mode

Default Configuration

The default for owner is 255 and for non-owner it is 100.

User Guidelines

The priority of the owner cannot be changed. It is always 255.

Example

The following example shows how to set VRRP priority:

```
switchxxxxxx(config)# interface vlan 10
switchxxxxxx(config-if)# vrrp 1 priority 110
switchxxxxxx(config-if)# exit
```

61.8. vrrp shutdown

To disable the VRRP virtual router on the interface (meaning that it changes its status to Initialize), use the `vrrp shutdown` command in Interface Configuration mode. To return to the default, use the no format of the command.

Syntax

- vrrp vrid shutdown
- no vrrp vrid shutdown

Parameters

- vrid - Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.

Default Configuration

Disabled.

Command Mode

Interface Configuration mode

User Guidelines

When a VRRP virtual router is disabled on an interface, its configuration is not removed.

Example

The following example shows how to enable a specified virtual router:

```
switchxxxxxx(config)# interface vlan 10
switchxxxxxx(config-if)# no vrrp 1 shutdown
switchxxxxxx(config-if)# exit
```

61.9. vrrp source-ip

To define a real VRRP address that will be used as the source IP address of VRRP messages, use the `vrrp source-ip` command in Interface Configuration mode. To return to the default, use the no format of the command.

Syntax

- vrrp vrid source-ip ip-address

- no vrrp vrid source-ip

Parameters

- vrid - Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.
- ip-address - VRRP router's IP address: one of IP addresses of VRRP router defined on the same interface.

Default Configuration

Lowest VRRP router's IP address defined on the interface.

Command Mode

Interface Configuration mode

User Guidelines

Example

The following example shows how to define a source ip address to the specified VRRP virtual router:

```
switchxxxxxx(config)# interface vlan 10
switchxxxxxx(config-if)# vrrp 1 source-ip 192.168.2.1
switchxxxxxx(config-if)# exit
```

61.10. vrrp timers advertise

To define the interval between successive advertisements by the Master VRRP virtual router, use the `vrrp timers advertise` command in Interface Configuration mode. To return to the default, use the no format of the command.

Syntax

- vrrp vrid timers advertise [msec] interval
- no vrrp vrid timers advertise

Parameters

- vrid - Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.
- msec - (Optional) Changes the unit of the advertisement time from seconds to milliseconds. Without the keyword, the advertisement interval is in seconds.
- interval - Time interval between successive advertisements. If keyword msec is present then the valid range is 50 to 40950 milliseconds. If keyword msec is omitted then the valid range is 1 to 40 seconds.

Command Mode

Interface Configuration mode

Default Configuration

1 second

User Guidelines

If the advertisement interval is configured in msec, the operation advertisement interval will be the configured advertisement interval round down to the nearest seconds for VRRP v2 and to the nearest centiseconds (10ms) for VRRP v3.

Example

The following example shows how to set VRRP timer advertise of 500 msec to specified VRRP virtual router:

```
switchxxxxxx(config)# interface vlan 10
switchxxxxxx(config-if)# vrrp 1 timers advertise msec 500
switchxxxxxx(config-if)# exit
```

61.11. vrrp version

To define the supported VRRP version, use the `vrrp version` command in Interface Configuration mode. To return to the default, use the no format of the command.

Syntax

- vrrp vrid version 2 | 3 | 2&3
- no vrrp vrid version

Parameters

- vrid - Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.
- 2 - VRRPv2 specified by RFC3768 is supported. Received VRRPv3 messages are dropped by the VRRP virtual router. Only VRRPv2 advertisements are sent.
- 3 - VRRPv3 specified by RFC5798 is supported without VRRPv2 support (8.4, RFC5798). Received VRRPv2 messages are dropped by the VRRP virtual router. Only VRRPv3 advertisements are sent.
- 2&3 - VRRPv3 specified by RFC5798 is supported with VRRPv2 support (8.4, RFC5798). Received VRRPv2 messages are treated by the VRRP virtual router. VRRPv3 and VRRPv2 advertisements are sent.

Default Configuration

Version 2.

Command Mode

Interface Configuration mode

User Guidelines

Version 2&3 is intended for upgrade scenarios and is not for permanent deployment. Please refer to VRRP 3 standard for version 2 and version 3 interoperability.

Example

The following example shows how to define VRRP version to specified VRRP virtual router:

```
switchxxxxxx(config)# interface vlan 10
switchxxxxxx(config-if)# vrrp 1 version 2
switchxxxxxx(config-if)# exit
```

62. Web Server Commands

62.1. ip https certificate

To configure the active certificate for HTTPS, use the `ip https certificate` Global Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- ip https certificate number
- no ip https certificate

Parameters

- number - Specifies the certificate number. (Range: 1–2)

Default Configuration

The default certificate number is 1.

Command Mode

Global Configuration mode

User Guidelines

First, use `crypto certificate generate` to generate one or two HTTPS certificates. Then use this command to specify which is the active certificate.

Example

The following example configures the active certificate for HTTPS.

```
switchxxxxxx(config)# ip https certificate 2
```

62.2. ip http port

To specify the TCP port used by the web browser interface, use the `ip http port` Global Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- ip http port port-number
- no ip http port

Parameters

- port port-number - For use by the HTTP server. (Range: 1–65534)

Default Configuration

The default port number is 80.

Command Mode

Global Configuration mode

Example

The following example configures the http port number as 100.

```
switchxxxxxx(config)# ip http port 100
```

62.3. ip http server

To enable configuring and monitoring the device from a web browser, use the `ip http server` Global Configuration mode command. To disable this function, use the no form of this command.

Syntax

- ip http server
- no ip http server

Parameters

This command has no arguments or keywords.

Default Configuration

HTTP server is enabled for access from up to 4 users at once.

Command Mode

Global Configuration mode

Example

The following example enables configuring the device from a web browser.

```
switchxxxxxx(config)# ip http server
```

62.4. ip http secure-server

To enable the device to be configured or monitored securely from a browser, use the `ip http secure-server` Global Configuration mode command. To disable this function, use the no form of this command.

Syntax

- ip http secure-server
- no ip http secure-server

Parameters

This command has no arguments or keywords.

Default Configuration

HTTPS server is enabled for access from up to 4 users at once.

Command Mode

Global Configuration mode

User Guidelines

After this command is used, you must generate a certificate using `crypto certificate generate`. If no certificate is generated, this command has no effect.

Example

```
switchxxxxxx(config)# ip http secure-server
```

62.5. ip http secure-port

To specify the TCP port to be used by the secure web browser, use the `ip http secure-port` Global Configuration mode command. To use the default port, use the no form of this command.

Syntax

- ip http secure-port port-number
- no ip http secure-port

Parameters

- port-number - Port number for use by the HTTPS server (Range: 1–65534)

Default Configuration

The default port number is 443.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# ip http secure-port 1234
```

62.6. ip http timeout-policy

To set the interval for the system to wait for user input in http/https sessions before automatic logoff, use the `ip http timeout-policy` Global Configuration mode command. To return to the default value, use the no form of this command.

Syntax

- ip http timeout-policy idle-seconds [{http-only | https-only}]
- no ip http timeout-policy

Parameters

- idle-seconds - Specifies the maximum number of seconds that a connection is kept open if no data is received or response data cannot be sent out. (Range: 0–86400)
- http-only - (Optional) The timeout is specified only for http
- https-only - (Optional) The timeout is specified only for https

Default Configuration

600 seconds

Command Mode

Global Configuration mode

User Guidelines

To specify no timeout, enter the ip http timeout-policy 0 command.

Example

The following example configures the http timeout to be 1000 seconds.

```
switchxxxxxx(config)# ip http timeout-policy 1000
```

62.7. show ip http

To display the HTTP server configuration, use the `show ip http` Privileged EXEC mode command.

Syntax

- show ip http

Parameters

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

Example

The following example displays the HTTP server configuration.

```
switchxxxxxx# show ip http
HTTP server enabled
Port: 80
Interactive timeout: 10 minutes
```

62.8. show ip https

To display the HTTPS server configuration, use the `show ip https` Privileged Privileged EXEC mode command.

Syntax

- show ip https

Parameters

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

Example

The following example displays the HTTPS server configuration.

```
switchxxxxxx# show ip https
HTTPS server enabled
Port: 443
Interactive timeout: Follows the HTTP interactive timeout (10 minutes)
Certificate 1 is active
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
Certificate 2 is inactive
Issued by: self-signed
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: 1873B936 88DC3411 BC8932EF 782134BA
```

MICROSENS

Disclaimer

All information in this document is provided ‘as is’ and is subject to change without notice.

MICROSENS GmbH & Co. KG disclaims any liability for the correctness, completeness or quality of the information provided, fitness for a particular purpose or ensuing damage.

Any product names mentioned herein may be trademarks and/or registered trademarks of their respective owners.

Document ID: PM_19001_2022-03-24