Cisco Catalyst PON Series Switches OLT Command Reference

First Published: 2020-11-09

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Using the Command-Line Interface

This chapter contains the following topics:

Using the Command-Line Interface

This chapter describes the command-line interface (CLI) and how to use it to configure your device.

Understanding Command Modes

The user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

When you start a session on the switch, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the switch reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you can enter any privileged EXEC command or enter global configuration mode.

Using the configuration modes (global and interface), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the device reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode.

This table describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode. The examples in the table use the hostname *Device*.

Table 1: Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your device.	`Device>`	Enter **exit** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information.

Mode	Access Method	Prompt	Exit Method	About This Mode
Privileged EXEC	While in user EXEC mode, enter the **enable** command.	`Device#`	Enter **exit** to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the **configure** command.	`Device(config)#`	To exit to privileged EXEC mode, enter **exit** or **end**, or press **Ctrl-Z**.	Use this mode to configure parameters that apply to the entire switch.
Ethernet interface configuration	While in global configuration mode, enter the **interface ethernet** command (with a specific interface).	`Device(config-if-ethernet-1/1)#`	To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure parameters for the Ethernet ports.
VLAN configuration	While in global configuration mode, enter the **vlan** *vlan-id* command.	`Device(config-if-vlan)#`	To exit to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure VLAN parameters.
AAA configuration	While in global configuration mode, enter the **aaa** command.	`Device(config-aaa)#`	To exit to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to setup the domain.

Mode	Access Method	Prompt	Exit Method	About This Mode
RADIUS configuration	While in global configuration mode, enter the **radius host** *radius-name* command.	`Device(config-radius-r1)#`	To exit to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure RADIUS parameters.
VLAN interface configuration	While in global configuration mode, enter the **interface vlan-interface** *vlan-id* command.	`Device(config-if-vlaninterface-22)#`	To exit to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure VLAN Layer 3 interface

Understanding the Help System

You can enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command.

Table 2: Help Summary

Command	Purpose
help	Obtains a brief description of the help system in any command mode.

abbreviated-command-entry **?**
`Device# cl?`
`clear clock cls`
	Obtains a list of commands that begin with a particular character string.

abbreviated-command-entry <Tab>
`Device# sh cl<tab>`
`Device# show clock`
	Completes a partial command name.

? `Device> ?`	Lists all commands available for a particular command mode.

Command	Purpose
command **?** `Device show ?`	Lists the associated keywords for a command.

command keyword **?**
 	
`Device(config)# clock timezone ?`
`STRING<1-32>  name of timezone`
	Lists the associated arguments for a keyword.

Understanding Abbreviated Commands

You need to enter only enough characters for the switch to recognize the command as unique.

This example shows how to enter the **show version** command in an abbreviated form:

```
Device# show ver
```

Understanding no Forms of Commands

Almost every configuration command also has a **no** form. In general, use the **no** form to disable a feature or function or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to re-enable a disabled feature or to enable a feature that is disabled by default.

Understanding CLI Error Messages

This table lists some error messages that you might encounter while using the CLI to configure your device.

Table 3: Common CLI Error Messages

Error Message	Meaning	How to Get Help
`% Incomplete command.`	You did not enter all the keywords or values required by this command.	Re-enter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
`% Invalid input detected at '^' marker.`	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The possible keywords that you can enter with the command appear.

Using Editing Features

This section describes the editing features that can help you manipulate the command line.

Editing Commands through Keystrokes

This table shows the keystrokes that you need to edit command lines. These keystrokes are optional.

Note The arrow keys function only on ANSI-compatible terminals such as VT100s.

Table 4: Editing Commands through Keystrokes

Capability	Keystroke	Purpose
Move around the command line to make changes or corrections.	Press **Ctrl-B**, or press the left arrow key.	Moves the cursor back one character.
	Press **Ctrl-F**, or press the right arrow key.	Moves the cursor forward one character.
	Press **Ctrl-A**.	Moves the cursor to the beginning of the command line.
	Press **Ctrl-E**.	Moves the cursor to the end of the command line.
	Press **Esc B**.	Moves the cursor back one word.
	Press **Esc F**.	Moves the cursor forward one word.
	Press **Ctrl-T**.	Transposes the character to the left of the cursor with the character located at the cursor.
Recall commands from the buffer and paste them in the command line. The switch provides a buffer with the last ten items that you deleted.	Press **Ctrl-Y.**	Recalls the most recent entry in the buffer.
	Press **Esc Y**.	Recalls the next buffer entry. The buffer contains only the last 10 items that you have deleted or cut. If you press **Esc Y** more than ten times, you cycle to the first buffer entry.
Delete entries if you make a mistake or change your mind.	Press the **Delete** or **Backspace** key.	Erases the character to the left of the cursor.

Capability	Keystroke	Purpose
	Press **Ctrl-D**.	Deletes the character at the cursor.
	Press **Ctrl-K**.	Deletes all characters from the cursor to the end of the command line.
	Press **Ctrl-U** or **Ctrl-X**.	Deletes all characters from the cursor to the beginning of the command line.
	Press **Ctrl-W**.	Deletes the word to the left of the cursor.
	Press **Esc D**.	Deletes from the cursor to the end of the word.
Capitalize or lowercase words or capitalize a set of letters.	Press **Esc C**.	Capitalizes at the cursor.
	Press **Esc L**.	Changes the word at the cursor to lowercase.
	Press **Esc U**.	Capitalizes letters from the cursor to the end of the word.
Designate a particular keystroke as an executable command, perhaps as a shortcut.	Press **Ctrl-V** or **Esc Q**.	
Scroll down a line or screen on displays that are longer than the terminal screen can display. **Note** The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including **show** command output. You can use the **Return** and **Space** bar keystrokes whenever you see the More prompt.	Press the **Return** key.	Scrolls down one line.
	Press the **Space** bar.	Scrolls down one screen.
Redisplay the current command line if the switch suddenly sends a message to your screen.	Press **Ctrl-L** or **Ctrl-R**.	Redisplays the current command line.

Editing Command Lines that Wrap

You can use a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten

characters of the line, but you can scroll back and check the syntax at the beginning of the command. The keystroke actions are optional.

To scroll back to the beginning of the command entry, press **Ctrl-B** or the left arrow key repeatedly. You can also press **Ctrl-A** to immediately move to the beginning of the line.

Note The arrow keys function only on ANSI-compatible terminals such as VT100s.

In this example, the **access-list** global configuration command entry extends beyond one line. When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign ($) shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.

```
Device(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
Device(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
Device(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
Device(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

After you complete the entry, press **Ctrl-A** to check the complete syntax before pressing the **Return** key to execute the command. The dollar sign ($) appears at the end of the line to show that the line has been scrolled to the right:

```
Device(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1$
```

The software assumes that you have a terminal screen that is 80 columns wide. If you have a width other than that, use the **terminal width** privileged EXEC command to set the width of your terminal.

Use line wrapping with the command history feature to recall and modify previous complex command entries.

Searching and Filtering Output of show and more Commands

You can search and filter the output for **show** and **more** commands. This is useful when you need to sort through large amounts of output or if you want to exclude output that you do not need to see. Using these commands is optional.

To use this functionality, enter a **show** or **more** command followed by the pipe character (|), one of the keywords **begin**, **include**, or **exclude**, and an expression that you want to search for or filter out:

command | {**begin** | **include** | **exclude**} *regular-expression*

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* appear.

This example shows how to include in the output display only lines where the expression *protocol* appears:

```
Device# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
GigabitEthernet1/0/1 is up, line protocol is down
GigabitEthernet1/0/2 is up, line protocol is up
```

Accessing the CLI through a Console Connection or through Telnet

Before you can access the CLI, you must connect a terminal or a PC to the device console or connect a PC to the Ethernet management port and then power on the device, as described in the hardware installation guide that shipped with your device.

CLI access is available before device setup. After your device is configured, you can access the CLI through a remote Telnet session or SSH client.

You can use one of these methods to establish a connection with the device:

- Connect the device console port to a management station or dial-up modem, or connect the Ethernet management port to a PC. For information about connecting to the console or Ethernet management port, see the device hardware installation guide.
- Use any Telnet TCP/IP or encrypted Secure Shell (SSH) package from a remote management station. The device must have network connectivity with the Telnet or SSH client, and the device must have an enable secret password configured.

  The device supports up to 16 simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.

  The device supports up to five simultaneous secure SSH sessions.

After you connect through the console port, through the Ethernet management port, through a Telnet session or through an SSH session, the user EXEC prompt appears on the management station.

New and Changed Information

New and Changed Information

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Modification
OLT v1.2.2.0	The following commands are deprecated: • **sntp client summer-time daily** • **sntp client summer-time weekly** The following changes are introduced for the **sip user mode** command: • New keywords **primary-dns** and **secondary-dns** added to replace the bias terms. • The *host id* for a unique profile is fixed at a value of 1. The **gemport** command has a new **encrypt** keyword.

Release	Modification
	The following commands are introduced: • **clock summer-time** • **clear dhcpv6 snooping** • **dhcpv6 snooping** • **dhcpv6 snooping max-clients** • **dhcpv6 snooping port down action fast remove** • **dhcpv6 snooping trust** • **show dhcpv6 snooping clients** • **show dhcpv6 snooping interface** • **show dhcpv6 snooping vlan** • **host-guard bind ip** • **ntp access** • **ntp authentication** • **ntp max-dynamic-sessions** • **ntp reference-clock** • **ntp unicast** • **show ntp access** • **show ntp authentication** • **show ntp broadcast-server** • **show ntp disable** • **show ntp max-dynamic-sessions** • **show ntp multicast-server** • **show ntp reference-clock** • **show ntp sessions** • **show ntp status** • **show ntp unicast-peer** • **show ntp unicast-server** • **mld-snooping** • **mld-snooping host-aging-time** • **mld-snooping fast-leave**

Release	Modification
	• **mld-snooping group-limit** • **mld-snooping {permit|deny}** • **mld-snooping querier** • **mld-snooping query-interval** • **mld-snooping query-max-respond** • **mld-snooping querier-vlan** • **mld-snooping route-port forward** • **mld-snooping max-response-time** • **mld-snooping multicast vlan** • **mld-snooping record-host** • **mld-snooping route-port** • **mld-snooping router-port-age** • **show mld-snooping** • **show mld-snooping router-dynamic** • **show mld-snooping router-static** • **show multicast mld-snooping interface** • **show running-config mld_snooping**

Release	Modification
	• **ipv6 address** • **ipv6 address link-local** • **ipv6 enable** • **ipv6 icmpv6 multicast-echo-reply** • **ipv6 nd dad attempts** • **ipv6 nd ns retrans-time** • **ipv6 nd reachable-time** • **ipv6 neighbors max-learning-num** • **ipv6 path** • **ipv6 route** • **no ipv6 neighbor** • **show ipv6 interface** • **show ipv6 nd dad attempts** • **show ipv6 nd ns retrans-time** • **show ipv6 nd reachable-time** • **show ipv6 neighbors** • **show ipv6 route**
OLT v1.2.1.17	Introductory release for OLT.

PART I

Getting Started With OLT Network

Getting Started With OLT Network

add inner-vlan

To configure VLAN stacking rule, use the **add inner-vlan** command in VLAN profile configuration mode. To delete the VLAN stacking rule, use the **no add inner-vlan** command.

add inner-vlan *inner-vlan-id* {*priority* | **outer-vlan** *outer-vlan-id* [*priority*]}

no add inner-vlan *inner-vlan-id* [*priority*]

Syntax Description

inner-vlan-id	The inner VLAN ID. The range is from 0 to 4094.
outer-vlan-id	The outer VLAN ID. The range is from 0 to 4094.
priority	The 802.1 priority value. The range is from 0 to 7.

Command Modes

VLAN profile configuration (deploy-profile-vlan)

Usage Guidelines

A VLAN profile type must be configured.

Modifying and activating the VLAN template will cause the ONT that references the template to go online again.

Examples

This example shows how to configure VLAN stacking rule.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile vlan
Device(deploy-profile-vlan)# aim 5
Device(deploy-profile-vlan-5)# add inner-vlan 2 3 outer-vlan 2 3
Device(deploy-profile-vlan-5)# active
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

aim

To create profile based aim. use the **aim** command in profile configuration mode.

For alarm, dba, line, downstream traffic, upstream traffic and VLAN profile configuration modes

aim {*index_number* | **name** *name*}

For rule and unique profile configuration modes

aim {*slot-num/pon-num/ont-num* | **name** *name*}

Syntax Description

index_number	The profile index number. The range is from 0 to 1023.
name	The profile name. The format is string. The string length range is from 1 to
slot-num/pon-num/ont-num	The ONT ID. • *slot-num*: The slot number. The value is 0. • *pon-num*: The PON number. The range is from 1 to • *ont-num*: The ONT number. The range is from 1 to

Command Modes

Profile configuration (deploy-profile)

Usage Guidelines

A profile type must be configured.

Examples

This example shows how to create a VLAN aim.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile vlan
Device(deploy-profile-vlan)# aim 5
Device(deploy-profile-vlan-5)#
```

Example

This example shows how to create a unique aim.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile unique
Device(deploy-profile-unique)# aim 0/1/1
Device(deploy-profile-unique-0/1/1)#
```

Related Commands

Command	Description
delete aim	Deletes profile based aim.

alarm ont register-record

To enable ONT register record alarm and set an alarm threshold, use the **alarm ont register-record** command in global configuration mode. To disable the alarm, use the **no alarm ont register-record** command.

alarm ont register-record [**threshold**]*threshold_value*

no alarm ont register-record [**threshold**]*threshold_value*

Syntax Description

threshold_value	The threshold value. The range is from 1 to 128. The default is 64.

Command Modes

Global configuration (config)

Usage Guidelines

You can limit the number of ONTs that can be registered on the PON port by setting a threshold value. If the number of ONTs on the PON port exceeds the threshold value, an alarm is generated. The alarm is cancelled once the number of ONTs is less than the threshold value.

Examples

This example shows how to set an ONT register record alarm threshold value.

```
Device> enable
Device# configure terminal
Device(config)# alarm ont register-record threshold 80
```

Related Commands

Command	Description
show alarm ont register-record	Displays information about register record alarm of an ONT

crypto key

To configure or remove a key, use the **crypto key** command in privileged EXEC mode.

crypto key {**generate rsa** | **refresh** | **zeroize rsa**}

Syntax Description

generate rsa	Configures a default key.
refresh	Activates the key.
zeroize rsa	Removes the key.

Command Modes

Privileged EXEC (#)

Usage Guidelines

SSH must be enabled on the device.

Examples

This example shows how to configure a default key.

```
Device> enable
Device# crypto key generate rsa
Generate default SSH key successfully.
```

This example shows how to activate the key.

```
Device> enable
Device# crypto key refresh
Refresh SSH key successfully.
```

Example

This example shows how to remove the key.

```
Device> enable
Device# crypto key zeroize rsa
Zeroize SSH key successfully.
```

Related Commands

Command	Description
ssh	Enables SSH on an OLT.

default vlan

To configure the VLAN tagging rule, use the **default vlan** command in VLAN profile configuration mode. To delete the VLAN tagging rule, use the **no default vlan** command.

default vlan *vlan_id* [*priority*]

Syntax Description

vlan_id	The VLAN ID. The range is from 1 to 4094.
priority	The 802.1 priority value. The range is from 0 to 7.

Command Modes

VLAN profile configuration (deploy-profile-vlan)

Usage Guidelines

A VLAN profile type must be configured.

Modifying and activating the VLAN template will cause the ONT that references the template to go online again.

Examples

This example shows how to configure the VLAN tagging rule.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile vlan
Device(deploy-profile-vlan)# aim 5
Device(deploy-profile-vlan-5)# default vlan 5 5
Device(deploy-profile-vlan-5)# active
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

delete aim

To delete profile based aim, use the **delete aim** command in profile configuration mode.

For alarm, dba, line, downstream traffic, upstream traffic and VLAN profile configuration modes

delete aim {*profile_list* | **name** *name*}

For rule and unique profile configuration modes

delete aim {*slot-num/pon-num/ont-num* | **name** *name*}

Syntax Description

index_number	The profile index number. The range is from 0 to 1023.
name	The profile name. The format is string. The string length range is fr
slot-num/pon-num/ont-num	The ONT ID. • *slot-num*: The slot number. The value is 0. • *pon-num*: The PON number. The range is fr • *ont-num*: The ONT number. The range is fr

Command Modes

Profile configuration (deploy-profile)

Usage Guidelines

A profile type and profile based aim must be created on the device.

Examples

This example show how to delete a VLAN aim configuration.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile vlan
Device(deploy-profile-vlan)# delete aim 5
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

deploy profile

To deploy a profile type, use the **deploy profile** command in global configuration mode.

deploy profile {**alarm** | **dba** | **ds-traffic** | **line** | **rule** | **unique** | **us-traffic** | **vlan**}

Syntax Description

alarm	The alarm profile.
dba	The DBA profile.
ds-traffic	The downstream traffic profile.
line	The line profile.
rule	The rule profile.
unique	The unqiue profile.
us-traffic	The upstream traffic profile.
vlan	The VLAN profile.

Command Modes

Global configuration (config)

Examples

This example shows how to deploy a line profile.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
```

Related Commands

Command	Description
aim	Creates aim based on the profile.

description

To configure an ONT description, use the **description** *ont_description* command in unique profile configuration mode. To delete an ONT description, use the **no description** *ont_description* command.

description *ont_description*

no description *ont_description*

Syntax Description

ont_description	The ONT description.

Command Modes

Unique profile configuration (deploy-profile-unique)

Usage Guidelines

A unique profile type must be configured.

Examples

This example shows how to configure an ONT description.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile unique
Device(deploy-profile-unique)# aim 0/1/1
Device(deploy-profile-unique-0/1/1)# description cisco
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

device type

To configure a device type, use the **device type** *type* command in line profile configuration mode.

device type *type*

Syntax Description

type	The ONT device type name. The name of the ONT device type should conform Specification formulated.

Command Modes

Line profile configuration (deploy-profile-line)

Usage Guidelines

A line profile type must be configured.

Modifying and activating the line traffic profile will cause the ONT that references the template to go online again.

Examples

This example shows how to configure a device type.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 5
Device(deploy-profile-line-5)# device type c40-100
Device(deploy-profile-line-5)# active
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

ds car bandwidth

To configure committed access rate (CAR) downlink of a GEM port, use the **ds car bandwidth** command in downlink traffic profile configuration mode.

ds car bandwidth *bandwidth_rate*

Syntax Description

bandwidth_rate	The downstream bandwidth in kbps. The value range is from 64 to 2608832.

Command Modes

Downlink traffic profile (deploy-profile-ds-traffic)

Usage Guidelines

A downlink profile type must be configured.

Modifying and activating the downlink traffic profile will cause the ONT that references the template to go online again.

Examples

This example shows how to configure a GEM port

```
Device> enable
Device# configure terminal
Device(config)# deploy profile ds-traffic
Device(deploy-profile-ds-traffic)# aim 5
Device(deploy-profile-ds-traffic-5)# ds car bandwidth 1024
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

flow port default

To create a default flow rule, use the **flow** *flow_id* **port** {**eth** *port-id* | **veip** | **iphost**} **default** command. To delete a default VLAN flow rule, use the **no** form of this command.

flow *flow_id* **port** {**eth** *port-id* | **veip** | **iphost**} **default vlan** *destination_vlan_id* [*priority*]

no flow *flow_id*

Syntax Description

flow_id	The flow index. The range is from 0 to 63.
port-id	The ONT Ethernet port ID. The range is from 1 to 24.
default	Specifies the default configuration.
destination_vlan_id	The destination VLAN ID The range is from 1 to 4094.
priority	The VLAN priority. The range is from 0 to 7.

Command Modes

Line profile configuration (deploy-profile-line)

Usage Guidelines

A line profile type must be configured.

Modifying and activating the line traffic profile will cause the ONT that references the template to go online again.

Examples

This example shows how to create a default VLAN flow rule.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 5
Device(deploy-profile-line-5)# flow 2 port eth 3 default vlan 3 3
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

flow port etype

To create a flow rule based on ethernet frame type, use the **flow** *flow_id* **port** {**eth** *port-id* | **veip** | **iphost**} **etype** command. command. To delete a flow rule based on ethernet frame type, use the **no** form of this command.

flow *flow_id* **port** {**eth** *port-id* | **veip** | **iphost**} **etype** {**arp** | **ipoe** | **pppoe**} {**default vlan** *source_vlan_id priority* | **transparent** | **vlan** *source_vlan_id* {*priority* | **add vlan** *destination_vlan_id* [*priority*] | **keep** | **translate vlan** *destination_vlan_id* [*priority*]}}

no flow *flow_id*

Syntax Description

flow_id	The flow index. The range is from 0 to 63.
port-id	The ONT Ethernet port ID. The range is from 1 to 24.
default	Specifies the default configuration.
destination_vlan_id	The destination VLAN ID The range is from 1 to 4094.
priority	The VLAN priority. The range is from 0 to 7.
etype	Specifies user ethernet frame type a
arp	Specifies ARP as the filter type.
ipoe	Specifies IPoE as the filter type.
pppoe	Specifies PPPOE as the filter type.
source_vlan_id	The source VLAN ID The range is from 1 to 4094.
transparent	Specifies the service type as transpa
add	Adds outer service VLAN
keep	Adds trunk as the service type.
translate	Add translate as the service type.

Command Modes

Line profile configuration (deploy-profile-line)

Usage Guidelines

A line profile type must be configured.

Modifying and activating the line traffic profile will cause the ONT that references the template to go online again.

Examples

This example shows how to create a translate flow rule based on ethernet frame type.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 5
Device(deploy-profile-line-5)# flow 2 port iphost etype arp vlan 3 translate vlan 4 1
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

flow port transparent

To create a transparent flow rule, use the **flow** *flow_id* **port** {**eth** *port-id* | **veip** | **iphost**} **transparent** command. To delete a transparent flow rule, use the **no** form of this command.

flow *flow_id* **port** {**eth** *port-id* | **veip** | **iphost**}**transparent**

no flow *flow_id*

Syntax Description

flow_id	The flow index. The range is from 0 to 63.
port-id	The ONT Ethernet port ID. The range is from 1 to 24.
transparent	Specifies the service type as transpa

Command Modes

Line profile configuration (deploy-profile-line)

Usage Guidelines

A line profile type must be configured.

Modifying and activating the line traffic profile will cause the ONT that references the template to go online again.

Examples

This example shows how to create a transparent flow rule.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 5
Device(deploy-profile-line-5)# flow 2 port eth 3 transparent
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

flow port vlan

To create a VLAN flow rule, use the **flow** *flow_id* **port** {**eth** *port-id* | **veip** | **iphost**} **vlan** command. To delete a VLAN flow rule, use the **no** form of this command.

flow *flow_id* **port** {**eth** *port-id* | **veip** | **iphost**} **vlan** *source_vlan_id* {*priority* | **add vlan** *destination_vlan_id* [*priority*] | **keep** | **translate vlan** *destination_vlan_id* [*priority*]}

no flow *flow_id*

Syntax Description

flow_id	The flow index. The range is from 0 to 63.
port-id	The ONT Ethernet port ID. The range is from 1 to 24.
destination_vlan_id	The destination VLAN ID The range is from 1 to 4094.
priority	The VLAN priority. The range is from 0 to 7.
source_vlan_id	The source VLAN ID The range is from 1 to 4094.
add	Adds outer service VLAN
keep	Adds trunk as the service type.
translate	Add translate as the service type.

Command Modes

Line profile configuration (deploy-profile-line)

Usage Guidelines

A line profile type must be configured.

Modifying and activating the line traffic profile will cause the ONT that references the template to go online again.

Examples

This example shows how to create a VLAN keep flow rule.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 5
Device(deploy-profile-line-5)# flow 2 port eth 3 vlan 2 keep
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

gemport

To create a GEM port and configure the parameters, use the **gemport** *gem_index* **tcont** *tcont_id* command in line profile configuration mode.

For line profile configuration mode

gemport *gem_index* **tcont** *tcont_id* { **encrypt** | **vlan-profile** | **us-traffic-profile** | **ds-traffic-profile** } { *index_number* | **name** *name* }

For unique profile configuration mode.

gemport *gem_index* {**vlan-profile** | **us-traffic-profile** | **ds-traffic-profile**} {*index_number* | **name** *name*}

Syntax Description

gem_index	The GEM port index number. The range is from 1 to 1024. Curren ports can be created in each line profile.
tcont_id	The T-CONT ID to bind to the GEM port. The range is from 1 to
encrypt	Enables Advanced Encryption Standard (AES) encryption
vlan-profile	The VLAN profile.
us-traffic-profile	The upstream traffic profile.
ds-traffic-profile	The downstream traffic profile.
index_number	The index of the template. The range is from 0 to M, where M is th of ONUs supported by the whole machine.
name	The name of the template.

Command Modes

Line profile configuration (deploy-profile-line)

Usage Guidelines

A line profile type must be configured.

Modifying and activating the line traffic profile causes the ONT that references the template to go online again.

Examples

This example shows how to create a gemport and configure a T-CONT to the gemport.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 5
GPON(deploy-profile-line-5)# device type n40-100-1
GPON(deploy-profile-line-5)# tcont 2 profile dba 1
Device(deploy-profile-line-5)# gemport traffic-mode car
Device(deploy-profile-line-5)# gemport 2 tcont 2 vlan-profile 1
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.
gemport traffic-mode	Configures the GEM traffic mode

gemport traffic-mode

To configure the GEM traffic mode, use the **gemport traffic-mode** command in line profile configuration mode.

gemport traffic-mode {**car** | **queue**}

Syntax Description

car	Specifies committed access rate (CAR) as GEM traffic mo
queue	Specifies priority scheduling queue as GEM traffic mode.

Command Modes

Line profile configuration (deploy-profile-line)

Usage Guidelines

A line profile type must be configured.

Modifying and activating the line traffic profile will cause the ONT that references the template to go online again.

Examples

This example shows how to configure the GEM port traffic mode based on queue.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 5
Device(deploy-profile-line-5)# gemport traffic-mode queue
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

load keyfile

To download the key from the external key server, use the **load keyfile** command in privileged EXEC mode.

Download from a TFTP server

load keyfile {**public** | **private**} **tftp** {**inet** | **inet6**}*server_ip filename*

Download from a FTP server

load keyfile {**public** | **private**} **ftp** {**inet** | **inet6**}*server_ip filename username password*

Syntax Description

public	The public SSH key file
private	The private SSH key file
tftp	Loads the file from the TFTP server.
ftp	Loads the file from FTP server.
inet	The IPv4 address family.
inet6	The IPv6 address family
server_ip	The server IP address
filename	The key filename.
username	The FTP username
password	The FTP password.

Command Modes

Privileged EXEC (#)

Usage Guidelines

SSH must be enabled on the device.

Examples

This example shows how to download the public key from the FTP server

```
Device> enable
Device# load keyfile public ftp inet 100.100.100.11 mykey admin 123456
```

Related Commands

Command	Description
ssh	Enables SSH on an OLT.
upload keyfile	Uploads the local key to the key server.

mapping

To create GEM port mapping, use the **mapping** *index_number* in line profile configuration mode. To disable GEM port mapping, use the **no mapping** *index_number* command.

mapping *index_number* {**port** {**eth** *port_id* | **veip** | **iphost**} | **priority** *priority_value* | **vlan** *vlan_id* }**gemport** *gemport_index*

no mapping *index_number*

Syntax Description

index_number	The mapping index number. The value range is from 0 to 47.
port_id	The ONT Ethernet port ID. The range is from 1 to 24.
eth	The ONT Ethernet interface. Optional for SFU
veip	The ONT WAN interface. Optional for HGU
iphost	The ONT voice IP interface.
gemport_index	The GEM Port index number. The ranges is from 1 to 1024. Currently, only 24 GEM Ports ca line profile.
priority	The 802.1P. The range is from 0 to 7.
vlan_id	The VLAN ID The range is from 1 to 4094.

Command Modes

Line profile configuration (deploy-profile-line)

Usage Guidelines

A line profile type must be configured.

Modifying and activating the line traffic profile will cause the ONT that references the template to go online again.

Examples

This example shows how to create GEM port mapping using ethernet port.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 5
Device(deploy-profile-line-5)# mapping 2 port eth 3 gemport 3
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

mapping mode

To configure the GEM port mapping mode, use the **mapping mode** command in line profile configuration mode.

mapping mode {**port** | **port-priority** | **port-vlan** | **port-vlan-priority** | **priority** | **vlan** | **vlan-priority**}

Syntax Description

port	Configures port as the mapping mode.
port-priority	Configures port and 802.1p priority as the mapping
port-vlan	Configures port and VLAN as the mapping mode
port-vlan-priority	Configures port, VLAN and 802.1p priority as the r
priority	Configures 802.1p priority as the mapping mode
vlan	Configures VLAN as the mapping mode
vlan-priority	Configures VLAN and 802.1p priority as the mappi

Command Modes

Line profile configuration (deploy-profile-line)

Usage Guidelines

A line profile type must be configured.

Modifying and activating the line traffic profile will cause the ONT that references the template to go online again.

Examples

This example shows how to configure the GEM port mapping mode as VLAN

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 5
Device(deploy-profile-line-5)# mapping mode vlan
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

no shutdown

To enable a shutdown port, use the **no shutdown** command in interface configuration mode. To disable a port use the **shutdown** command.

no shutdown

shutdown

Command Modes

Interface configuration (config-if)

Examples

This example shows how to enable a shutdown port.

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/1
Device(config-if-ethernet-1/1)# no shutdown
```

ont-find distance

To configure the ONT logical distance, use the **ont-find distance** command to global configuration mode. To disable the logical distance, use the **no ont-find distance** command.

ont-find distance min *minimum_distance* **max** *maximum_distance* **interface gpon** {*slot-number/port-number* | **all**}

no ont-find distance interface gpon {*slot-number/port-number* | **all**}

Syntax Description

min *minimum_distance*	The minimum distance. The range is from 0 to 40. The defau
max *maximum_distance*	The maximum distance. The distance range is from 0 to 60. T
slot-number/port-number	*slot-number/port-number* : The port • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is • 10GE Ethernet: The value • *port-number*: • GPON: The range is from • GE Ethernet: The range is • 10GE Ethernet: The range
all	All ports.

Command Modes

Global configuration (config)

Examples

This example shows how to configure the ONT logical distance.

```
Device> enable
Device# configure terminal
Device(config)# ont-find distance min 10 max 30 interface gpon 0/1
Change the logic distance will reset the PON port, are you sure(y/n)?[n]y
Config success: 1, failed: 0.
```

Related Commands

Command	Description
ont-find interface gpon	Enables auto-discover configuration.
ont-find interval-time	Configures the auto-discover interval time.

Command	Description
ont-find list-age	Configures the auto-discover aging time.
show ont-find config	Displays information about ONT auto find configuration and other related parameters.
show ont-find list	Displays information about ONT find list.

ont-find interface gpon

To enable auto-discover configuration, use the **ont-find interface gpon** command in global configuration mode. To disable the logical distance, use the **no ont-find interface gpon** command.

ont-find interface gpon {*slot-number/port-number* | **all**}

no ont-find interface gpon {*slot-number/port-number* | **all**}

Syntax Description

slot-number/port-number	*slot-number/port-number* : The port • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is • 10GE Ethernet: The value • *port-number*: • GPON: The range is from • GE Ethernet: The range is • 10GE Ethernet: The range
all	All ports.

Command Modes

Global configuration (config)

Examples

This example shows how to enable auto-discover configuration.

```
Device> enable
Device# configure terminal
Device(config)# ont-find interface gpon 0/1
```

Related Commands

Command	Description
ont-find distance	Configures the ONT logical distance.
ont-find interval-time	Configures the auto-discover interval time.
ont-find list-age	Configures the auto-discover aging time.
show ont-find config	Displays information about ONT auto find configuration and other related parameters.
show ont-find list	Displays information about ONT find list.

ont-find interval-time

To configure the auto-discover interval time, use the **ont-find interval-time** command in global configuration mode. To disable the auto-discover interval time, use the **no ont-find interval-time** command.

ont-find interval-time *interval_time* **interface gpon** {*slot-number/port-number* | **all**}

no ont-find interface gpon {*slot-number/port-number* | **all**}

Syntax Description

interval_time	The interval time. The range is from 3 to 30. Th
all	All ports.
slot-number/port-number	*slot-number/port-number* : The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1. • 10GE Ethernet: The value is 2. • *port-number*: • GPON: The range is from 1 to 8. • GE Ethernet: The range is from 1 to 4 • 10GE Ethernet: The range is from 1 t

Command Modes

Global configuration (config)

Examples

This example shows how to configure the ONT auto-discover interval time.

```
Device> enable
Device# configure terminal
Device(config)# ont-find interval-time 20 interface gpon 0/1
Config success: 1, failed: 0.
```

Related Commands

Command	Description
ont-find interface gpon	Enables auto-discover configuration.
ont-find distance	Configures the ONT logical distance.
ont-find list-age	Configures the auto-discover aging time.
show ont-find config	Displays information about ONT auto find configuration and other related parameters.
show ont-find list	Displays information about ONT find list.

ont-find list-age

To configure the auto-discover aging time, use the **ont-find list-age time** command in global configuration mode. Use the **no ont-find list-age time** command.

ont-find list-age time *aging_time* **interface gpon** {*slot-number/port-number* | **all**}

no ont-find list-age interface gpon {*slot-number/port-number* | **all**}

Syntax Description

aging_time	The discovery mode timeout time. The unit is hour. The valu 168.
slot-number/port-number	*slot-number/port-number* : The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1. • 10GE Ethernet: The value is 2. • *port-number*: • GPON: The range is from 1 to 8. • GE Ethernet: The range is from 1 to 4. • 10GE Ethernet: The range is from 1 to 2.
all	All ports.

Command Modes

Global configuration (config)

Examples

This example shows how to configure the auto-discover aging time.

```
Device> enable
Device# configure terminal
Device(config)# ont-find list-age time 600 interface gpon 0/1
Config success: 1, failed: 0.
```

Related Commands

Command	Description
ont-find interface gpon	Enables auto-discover configuration.
ont-find distance	Configures the ONT logical distance.
ont-find interval-time	Configures the auto-discover interval time.
show ont-find config	Displays information about ONT auto find configuration and other related parameters.

Command	Description
show ont-find list	Displays information about ONT find list.

ont-silent auth-fail

To enable the ONT auth-fail silent configuration, use the **ont-silent auth-fail** command in global configuration mode. To disable the ONT auth-fail silent configuration, use the **no ont-silent auth-fail** command.

ont-silent auth-fail {**time** *silence_period* | **interface gpon** {*slot-number/port-number* | **all**}}

no ont-silent auth-fail interface gpon {*slot-number/port-number* | **all**}

Syntax Description

silence_period	The silent period after a failed authentication. The unit in seconds. The range is from 1 to 86400. The d
slot-number/port-number	*slot-number/port-number* : The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1. • 10GE Ethernet: The value is 2. • *port-number*: • GPON: The range is from 1 to 8. • GE Ethernet: The range is from 1 to 4. • 10GE Ethernet: The range is from 1 to 2.
all	All ports.

Command Modes

Global configuration (config)

Examples

This example shows how to enable the ONT auth-fail silent configuration.

```
Device> enable
Device# configure terminal
Device(config)# ont-silent auth-fail time 40 interface gpon 0/1
Config success: 1, failed: 0.
```

Related Commands

Command	Description
ont-silent offline	Enables auto-discover configuration.

ont-silent offline

To enable the ONT offline silent configuration, use the **ont-silent offline** command in global configuration mode. To disable the ONT offline silent configuration, use the **no ont-silent offline** command.

ont-silent offline {**time** *silence_period* | **interface gpon** {*slot-number/port-number* | **all**}}

no ont-silent offline interface gpon {*slot-number/port-number* | **all**}

Syntax Description

silence_period	The silent period after a failed authentication. The unit in seconds. The range is from 1 to 86400. T
slot-number/port-number	*slot-number/port-number* : The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1. • 10GE Ethernet: The value is 2. • *port-number*: • GPON: The range is from 1 to 8. • GE Ethernet: The range is from 1 to 4. • 10GE Ethernet: The range is from 1 to 2.
all	All ports.

Command Modes

Global configuration (config)

Examples

This example shows how to enable the ONT offline silent configuration.

```
Device> enable
Device# configure terminal
Device(config)# ont-silent offline time 40 interface gpon 0/1
Config success: 1, failed: 0.
```

Related Commands

Command	Description
ont-silent auth-fail	Enables ONT auth-fail silent configuration

ont auto-config

To enable ONT auto-configuration, use the **ont auto-config** command in global configuration mode. To disable ONT auto-configuration, use the **no ont auto-config** command.

ont auto-config [*index_number* **name** *name* | **name** *name*] {**all-ont** | **device-type** *device_type*}

no ont auto-config [*index_number* **name** *name* | **name** *name*] {**all-ont** | **device-type** *device_type*}

Syntax Description

index_number	The index of the template. The range is from 0 to M, where number of ONUs supported by the whole machine.
name	The name of the template.
all-ont	All ONTs.
device-type *device_type*	The device identifier. The format is in string. The range is

Command Modes

Global configuration (config)

Examples

This example shows how to enable auto-configuration.

```
Device> enable
Device# configure terminal
Device(config)# ont auto-config
Device(config)# ont auto-config 1 device-type n40-428-1h line 1
```

permit loid-lopw

To creates a logical ONT ID and logical ONT ID password permit profile, use the **permit loid-lopw** command in rule profile configuration mode.

permit loid-lopw *lopw loid* **line** {*profile_line_list* | **name** *name*} {**default line** {*index_number* | **name** *name*} | **once-on** {**no-aging** | **aging-time** *time*}}

Syntax Description

lopw	The logical ONT ID password.
loid	The logical ONT ID.
profile_line_list	The profile line list number.
index_number	The profile index number. The range is from 0 to 1023.
name	The profile name. The format is string. The string len
no-aging	Configures no timeout for discover
aging-time *time*	Configures timeout for discovery r The unit is hour. The range is from

Command Modes

Rule profile configuration (deploy-profile-rule)

Usage Guidelines

A rule profile type must be configured.

Examples

This example shows how to create a logical ONT ID permit profile and logical ONT ID password permit profile.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile rule
Device(deploy-profile-rule)# aim 0/1/1
Device(deploy-profile-rule-0/1/1)# permit loid-lopw logical1 password1 line 1 default line
 1 once-on no-aging
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

permit loid

To create a logical ONT ID permit profile, use the **permit loid** command in rule profile configuration mode.

permit loid *loid* **line** {*profile_line_list* | **name** *name*} {**default line** {*index_number* | **name** *name*} | **once-on** {**no-aging** | **aging-time** *time*}}

Syntax Description

loid	The logical ONT ID.
profile_line_list	The profile line list number.
index_number	The profile index number. The range is from 0 to 1023.
name	The profile name. The format is string. The string length
no-aging	Configures no timeout for discovery m
aging-time *time*	Configures timeout for discovery mod The unit is hour. The range is from 1 t

Command Modes

Rule profile configuration (deploy-profile-rule)

Usage Guidelines

A rule profile type must be configured.

Examples

This example shows how to create a logical ONT ID permit profile.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile rule
Device(deploy-profile-rule)# aim 0/1/1
Device(deploy-profile-rule-0/1/1)# permit loid logical1 line 1 default line 1 once-on
no-aging
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

permit lopw

To create a logical ONT ID password permit profile, use the **permit lopw** command in rule profile configuration mode.

permit lopw *lopw* **line** {*profile_line_list* | **name** *name*} {**default line** {*index_number* | **name** *name*} | **once-on** {**no-aging** | **aging-time** *time*}}

Syntax Description

lopw	The logical ONT ID password.
profile_line_list	The profile line list number.
index_number	The profile index number. The range is from 0 to 1023.
name	The profile name. The format is string. The string len
no-aging	Configures no timeout for discover
aging-time *time*	Configures timeout for discovery r The unit is hour. The range is from

Command Modes

Rule profile configuration (deploy-profile-rule)

Examples

This example shows how to create a logical ONT ID password permit profile.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile rule
Device(deploy-profile-rule)# aim 0/1/1
Device(deploy-profile-rule-0/1/1)# permit lopw password1 line 1 default line 1 once-on
no-aging
```

permit pw

To create a password permit profile, use the **permit pw** command in rule profile configuration mode.

permit pw {**string** *string_password* | **hex** *hex_password*}**line** {*profile_line_list* | **name** *name*} {**default line** {*index_number* | **name** *name*} | **once-on** {**no-aging** | **aging-time** *time*}}

Syntax Description

string_password	The ONT password in Hex.
hex_password	The ONT password in string.
profile_line_list	The profile line list number.
index_number	The profile index number. The range is from 0 to 1023.
name	The profile name. The format is string. The string length
no-aging	Configures no timeout for discovery m
aging-time *time*	Configures timeout for discovery mod The unit is hour. The range is from 1 t

Command Modes

Rule profile configuration (deploy-profile-rule)

Usage Guidelines

A rule profile type must be configured.

Examples

This example shows how to create a password permit profile.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile rule
Device(deploy-profile-rule)# aim 0/1/1
Device(deploy-profile-rule-0/1/1)# permit pw string password1 line 1 default line 1
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

permit sn-pw

To create a serial number and password permit profile, use the **permit sn-pw** command in rule profile configuration mode.

permit sn-pw {**string-hex** *string_serial_number* | **hex** *hex_serial_number*} {**string** *string_password* | **hex** *hex_password*}**line** {*profile_line_list* | **name** *name*}**default line** {*index_number* | **name** *name*}

Syntax Description

hex_serial_number	The ONT serial number in Hex.
string_serial_number	The ONT serial number in string.
string_password	The ONT password in Hex.
hex_password	The ONT password in string.
profile_line_list	The profile line list number.
index_number	The profile index number. The range is from 0 to 1023.
name	The profile name. The format is string. The string leng

Command Modes

Rule profile configuration (deploy-profile-rule)

Usage Guidelines

A rule profile type must be configured.

Examples

This example shows how to create a serial number and password permit profile.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile rule
Device(deploy-profile-rule)# aim 0/1/1
Device(deploy-profile-rule-0/1/1)# permit sn-pw string-hex GPON-1790032e string password1
line 1 default line 1
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

permit sn

To create a serial number permit profile, use the **permit sn** command in rule profile configuration mode.

permit sn {**string-hex** *string_serial_number* | **hex** *hex_serial_number*}**line** {*profile_line_list* | **name** *name*}**default line** {*index_number* | **name** *name*}

Syntax Description

hex_serial_number	The ONT serial number in Hex.
string_serial_number	The ONT serial number in string.
profile_line_list	The profile line list number.
index_number	The profile index number. The range is from 0 to 1023.
name	The profile name. The format is string. The string length

Command Modes

Rule profile configuration (deploy-profile-rule)

Usage Guidelines

A rule profile type must be configured.

Examples

This example shows how to create a ONT serial number permit profile.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile rule
Device(deploy-profile-rule)# aim 0/1/1
Device(deploy-profile-rule-0/1/1)# permit sn string-hex GPON-1790032e line 1 default line
1
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

show alarm ont register-record

To display information about register record alarm of an ONT, use the **show alarm ont register-record** command in privileged EXEC or global configuration mode.

show alarm ont register-record

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view information about register record alarm of an ONT

```
Device> enable
Device# configure terminal
Device(config)# show alarm ont register-record
register ont record threshold alarm status : enable
register ont record threshold value        : 64
register ont record current value          :
gpon port 0/1 : 1(normal)
gpon port 0/2 : 0(normal)
gpon port 0/3 : 0(normal)
gpon port 0/4 : 0(normal)
gpon port 0/5 : 0(normal)
gpon port 0/6 : 0(normal)
gpon port 0/7 : 0(normal)
gpon port 0/8 : 0(normal)
```

show keyfile

To display the key file information, use the **show keyfile** command in privileged EXEC or global configuration mode.

show keyfile {**public** | **private**}

Syntax Description

public	The SSH public key file.
private	The SSH private key file.

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the key file information

```
Device> enable
Device# show keyfile public
```

show ont-find config

To display information about ONT auto find configuration, use the **show ont-find config** command in privileged EXEC or global configuration mode.

show ont-find config interface gpon {*port_list* | **all**}

Syntax Description

port_list	The GPON port.
all	All ports.

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view information about ONT auto find configuration.

```
Device> enable
Device# configure terminal
Device(config)# show ont-find config interface gpon 0/1
Port  Find    Find-interval  Age     Aging-time  D-min  D-max
g0/1  enable  10             enable  600         0      20
```

show ont-find list

To display information about ONT find list, use the **show ont-find list** command in privileged EXEC or global configuration mode.

show ont-find list {**interface gpon** {*slot-number/port-number* | **all**} | **sn** {**string-hex** *string_serial_number* | **hex** *hex_serial_number*}}

Syntax Description

slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1. • 10GE Ethernet: The value is • *port-number*: • GPON: The range is from 1 t • GE Ethernet: The range is fro • 10GE Ethernet: The range is
all	All ports.
hex_serial_number	The ONT serial number in Hex.
string_serial_number	The ONT serial number in string.

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view information about ONT find list

```
Device> enable
Device# configure terminal
Device(config)# show ont-find list interface gpon 0/1
```

show ont-silent config

To display information about ONT silent function, use the **show ont-silent config** command in privileged EXEC or global configuration mode.

show ont-silent config interface gpon {*port_list* | **all**}

Syntax Description

port_list	The GPON port.
all	All ports.

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the information about ONT silent function.

```
Device> enable
Device# configure terminal
Device(config)# show ont-silent config interface gpon 0/1
Port  Auth-fail  time  Offline  time
g0/1  enable     40    disable  -
```

show ont-silent list

To display information about silent ONT, use the **show ont-silent list** command in privileged EXEC or global configuration mode.

show ont-silent list {**interface gpon** {*slot-number/port-number* | **all**} | **sn** {**string-hex** *string_serial_number* | **hex** *hex_serial_number*}}

Syntax Description

slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1. • 10GE Ethernet: The value is • *port-number*: • GPON: The range is from 1 t • GE Ethernet: The range is fro • 10GE Ethernet: The range is
all	All ports.
hex_serial_number	The ONT serial number in Hex.
string_serial_number	The ONT serial number in string.

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the information about silent ONT.

```
Device> enable
Device# configure terminal
Device(config)# show ont-silent list interface gpon 0/1
```

show ont brief count

To display brief information about an ONT interface, use the **show ont brief count** command in privileged EXEC or global configuration mode.

show ont brief count interface interface gpon {*slot-number/port-number* | **all**}

Syntax Description

slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1. • 10GE Ethernet: The value is 2 • *port-number*: • GPON: The range is from 1 to • GE Ethernet: The range is fro • 10GE Ethernet: The range is f
all	All ports.

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the brief information about an ONT interface.

```
Device> enable
Device# configure terminal
Device(config)# show ont brief count interface gpon 0/1
Port  Online-num  Offline-num  Total
g0/1  1           4            5
Total entries: 1.
```

show ont description

To display the description of an ONT, use the **show ont description** command in privileged EXEC or global configuration mode.

show ont description {*slot-num/pon-num/ont-num* | **interface gpon** *slot-number/port-number* }

Syntax Description

slot-num/pon-num/ont-num	The ONT ID. • *slot-num*: The slot number. The value is 0. • *pon-num*: The PON number. The range is from 1 to • *ont-num*: The ONT number. The range is from 1 to
slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1. • 10GE Ethernet: The value is 2. • *port-number*: • GPON: The range is from 1 to 8. • GE Ethernet: The range is from 1 to 4. • 10GE Ethernet: The range is from 1 to 2.

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the description of an ONT

```
Device> enable
Device# configure terminal
Device(config)# show ont description interface gpon 0/1
```

show ont info

To display detailed information about an ONT, use the **show ont info** command in privileged EXEC or global configuration mode.

show ont info *slot-num/pon-num/ont-num*

Syntax Description

slot-num/pon-num/ont-num	The ONT ID. • *slot-num*: The slot number. The value is 0. • *pon-num*: The PON number. The range is fron • *ont-num*: The ONT number. The range is from

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view detailed information about an ONT

```
Device> enable
Device# configure terminal
Device(config)# show ont info 0/1/5
ONT                              :   0/1/5
Description                      :   -
TYPE                             :   -
Status                           :   online
Distance(m)                      :   3
Vendor ID                        :   CSCO
Software Version                 :   1.1.2.5/1.1.2.6
Firmware Version                 :   N40-428-1
Equipment ID                     :   4GE-POE-2POTS-CATV
SN                               :   GPON-5aa7012a
Password                         :   123456
LOID                             :   000a5aa7012a
LOID Password                    :   a7012a
Uplink PON ports                 :   1
ETH/POTS/TDM/MOCA ports          :   4/2/0/0
CATV ANI/UNI ports               :   0/1
T-CONTs/GEM ports                :   31/127
Traffic Schedulers               :   31
PQs in T-CONT 1-8                :   8/8/8/8/8/8/8/8
DBA method                       :   NSR
IP configuration                 :   not support
Type of flow control             :   GEMPORT CAR and PQ SCHEDULED
TX power cut off                 :   Not Support
Online/Offline time              :   05:04:03   2001/12/08
Up/Down time                     :   1 day(s) 17 hour(s) 34 minute(s)
```

show ssh

To display SSH configuration, use the **show ssh** command in privileged EXEC or global configuration mode.

show ssh

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the SSH configuration

```
Device> enable
Device# show ssh
ssh version  : 2.0
ssh state    : on
ssh key file : available
```

show ssh limit

To display the maximum number of the users, use the **show ssh limit** command in privileged EXEC or global configuration mode.

show ssh limit

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the maximum number of the users.

```
Device> enable
Device# show ssh limit
SSH user limit is 5, current is 0.
```

show telnet

To display the telnet information, use the **show telnet** command in privileged EXEC or global configuration mode.

show telnet

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to display the telnet information.

```
Device> enable
Device# configure terminal
Device(config)# show telnet
Telnet service port is 23, using port is 23, user limit is 5, current is 1.
```

sip agent

To configure the SIP proxy server, use the **sip agent proxy-server** command in unique profile configuration mode. To disable the SIP proxy server, use the **no sip agent proxy-server** command.

sip agent proxy-server *proxy_server_uri* {**outbound-proxy** | **registrar-server** | **signal-port** }*proxy_server_uri*

no sip agent

Syntax Description

proxy_server_uri	The proxy server URI.
outbound-proxy	The outbound proxy.
registrar-server	The registrar server.
signal-port	The signal port.

Command Modes

Unique profile configuration (deploy-profile-unique)

Usage Guidelines

A unique profile type must be configured.

Examples

This example shows how to configure the SIP proxy server.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile unique
Device(deploy-profile-unique)# aim 0/1/1
Device(deploy-profile-unique-0/1/1)# sip agent proxy-server 2
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

sip digitmap

To configure the SIP digit map, use the **sip digitmap** command in unique profile configuration mode.

sip digitmap dial-plan-id *dial_plan_id* **dial-plan-token** *token*

Syntax Description

dial_plan_id	The digit map index The range is from 1 to 10.
token	The token

Command Modes

Unique profile configuration (deploy-profile-unique)

Usage Guidelines

A unique profile type must be configured.

Examples

This example shows how to configure the SIP digit map.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile unique
Device(deploy-profile-unique)# aim 0/1/1
Device(deploy-profile-unique-0/1/1)# sip digitmap dial-plan-id 3 dial-plan-token token1
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

sip user

To configure the SIP users, use the **sip user** *user_id* command in unique profile configuration mode. To disable SIP users, use the **no sip user** *user_id* command.

sip user *pots_number* {**name** *username* **password** *password* | **telno** *telephone_number*}

no sip user *pots_number*

Syntax Description

pots_number	The ONT POTS port number. The value range is from 1 to 2
username	The SIP username. The username length is from 1 to 25.
password	The SIP password. The password length is from 1 to 25
telephone_number	The ONT local phone number. The digit length is from 1 to 25.

Command Modes

Unique profile configuration (deploy-profile-unique)

Usage Guidelines

A unique profile type must be configured.

Examples

This example shows how to configure the SIP users

```
Device> enable
Device# configure terminal
Device(config)# deploy profile unique
Device(deploy-profile-unique)# aim 0/1/1
Device(deploy-profile-unique-0/1/1)# sip user 2 name user 1 password 123
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

sip user mode

To configure a SIP inteface, use the **sip user mode** command in unique profile configuration mode. To disable a SIP interface, use the **no sip user mode** command.

sip user mode { **static ip-address** *ip_address* **mask** *mask* **gateway** *gateway_address* **primary-dns** *primary_dns_address* **secondary-dns** *secondary_dns_address* | **dhcp** } **vlan** *vlan_id* *priority* **host** *host_number*

no sip user mode

Syntax Description

ip-address *ip_address*	The IP addr
mask *mask*	The IP netw
gateway *gateway_address*	The gatewa
primary-dns *primary_dns_address*	The primary
secondary-dns *secondary_dns_address*	The seconda
vlan *vlan_id*	The VLAN The range is
priority	The priority The range is
host *host_number*	The host nu The host nu host.

Command Modes

Unique profile configuration (deploy-profile-unique)

Usage Guidelines

A unique profile type must be configured.

Examples

This example shows how to configure an SIP inteface

```
Device> enable
Device# configure terminal
Device(config)# deploy profile unique
Device(deploy-profile-unique)# aim 0/1/1
Device(deploy-profile-unique-0/1/1)# sip user mode dhcp vlan 2 4 host 1
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

snmp-server

To enable the snmp server to send traps or disable the snmp server, use the **snmp-server** command in global configuration mode.

snmp-server {**enable** | **disable**}

Syntax Description

enable	Enables the snmp server to send traps.
disable	Disables the snp server.

Command Modes

Global configuration (config)

Examples

This example shows how to disable the snmp server.

```
Device> enable
Device# configure terminal
Device(config)# snmp-server disable
```

ssh

To enable SSH, use the **ssh** command in global configuration mode. To disable SSH, use the **no ssh** command.

ssh

no ssh

Command Modes

Global configuration (config)

Examples

This example shows how to enable SSH.

```
Device> enable
Device# configure terminal
Device(config)# ssh
Config SSH state successfully.
```

Related Commands

Command	Description
ssh limit *value*	Limits the number of user logins on SSH.
stop vty {*vty_list* |**all**}	Removes logged in users.
crypto key	Configures or removes a key.
upload keyfile	Uploads the local key to the key server
load keyfile	Downloads the key from the external key server

ssh limit

To limit the number of user logins on SSH, use the **ssh limit** command in global configuration mode.

ssh limit *value*

Syntax Description

value	The user login limit value. The range is 0-5.

Command Modes

Global configuration (config)

Usage Guidelines

SSH must be enabled on the device.

Examples

This example shows how to limit the number of user logins on SSH.

```
Device> enable
Device# configure terminal
Device(config)# ssh limit 5
```

Related Commands

Command	Description
aim	Creates .

stop telnet client

To remove logged in Telnet clients, use the **stop telnet client** command in privileged EXEC mode.

stop telnet client {*terminal_id* | **all**}

Syntax Description

terminal_id	Telnet clients logged in through a particular termir
all	All Telnet clients.

Command Modes

Privileged EXEC (#)

Usage Guidelines

Use this command on the OLT configured as the Telnet server.

Examples

This example shows how to remove logged in Telnet clients

```
Device> enable
Device# stop telnet client all
Stop all telnet clients successfully.
```

Related Commands

Command	Description
telnet enable	Enables Telnet on a OLT and configures the OLT as the Telnet server.

stop vty

To remove logged in users, use the **stop vty** command in privileged EXEC mode.

stop vty {*vty_list* | **all**}

Syntax Description

vty_list	Users on the vty list only
all	All logged in users.

Command Modes

Privileged EXEC (#)

Usage Guidelines

SSH must be enabled on the device.

Examples

This example shows how to remove logged in users.

```
Device> enable
Device# stop vty 3
```

Related Commands

Command	Description
ssh	Enables SSH on an OLT.

tcont *tcont_id*

To create a transmission container (T-CONT), use the **tcont** *tcont_id* command in line profile configuration mode. To delete a T-CONT, use the **no tcont** *tcont_id* command.

tcont *tcont_id* **profile dba** {*index_number* | **name** *name*}

no tcont *tcont_id*

Syntax Description

tcont_id	The T-CONT ID. The range is from 1 to 8.
index_number	The index of the template. The range is from 0 to M, where M supported by the whole machine.
name	The name of the template.

Command Modes

Line profile configuration (deploy-profile-line)

Usage Guidelines

A line profile type must be configured.

Modifying and activating the line traffic profile will cause the ONT that references the template to go online again.

Examples

This example shows how to create a T-CONT.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 5
Device(deploy-profile-line-5)# tcont 6 profile dba 100
Device(deploy-profile-line-5)# active
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

telnet disable

To disable Telnet on an OLT, use the **telnet disable** command in global configuration mode.

telnet disable

Command Modes

Global configuration (config)

Usage Guidelines

Use this command on the OLT configured as the Telnet server.

Examples

This example shows how to disable Telnet on an OLT.

```
Device> enable
Device# configure terminal
Device(config)# telnet disable
```

Related Commands

Command	Description
telnet enable	Enables Telnet on a OLT and configures the OLT as the Telnet server.

telnet enable

To enable Telnet on an OLT and configures the OLT as the Telnet server , use the **telnet enable** command in global configuration mode.

telnet enable

Command Modes

Global configuration (config)

Examples

This example shows how to enable Telnet on an OLT

```
Device> enable
Device# configure terminal
Device(config)# telnet enable
```

Related Commands

Command	Description
telnet disable	Disables Telnet on an OLT.
telnet limit *value*	Limits the number of users that can login to the Telnet server.
timeout *value*	Enables the client timeout and configures the timeout value.
stop telnet client {*terminal_id* |**all**}	Removes logged in Telnet clients.

telnet limit

To limit the number of users that can login to the Telnet server, use the **telnet limit** command in global configuration mode.

telnet limit *value*

Syntax Description

value	The limit of the number of users. The range is 0-5.

Command Modes

Global configuration (config)

Usage Guidelines

Use this command on the OLT configured as the Telnet server.

Examples

This example shows how to limit the number of users that can login to the Telnet server.

```
Device> enable
Device# configure terminal
Device(config)# telnet limit 3
```

Related Commands

Command	Description
telnet enable	Enables Telnet on a OLT and configures the OLT as the Telnet server.

telnet *server-ip*

To login to the Telnet server, use the **telnet** *server-ip* command in Privileged EXEC mode.

telnet *server-ip* {*port-number* | **/localecho**}

Syntax Description

server-ip	The Telnet server IP address
port-number	The port number.
/localecho	

Command Modes

Privileged EXEC (#)

Examples

This example shows how to login to the Telnet server.

```
Device> enable
Device# telnet 100.100.100.1
```

Related Commands

Command	Description
telnetclient timeout *value*	Enables client timeout and configures the timeout interval.

telnetclient timeout

To enable client timeout , use the **telnetclient timeout** command in global configuration mode. To disable client timeout, use the **no telnetclient timeout** command.

telnetclient timeout [*value*]

no telnetclient timeout

Syntax Description

value	The system idle timeout value. The unit is minutes. The range is from 1 to 480.

Command Modes

Global configuration (config)

Usage Guidelines

Use this command on the OLT configured as the Telnet client. To enable client timeout, use the **telnetclient** command in global configuration mode. To configure the timeout interval, use the **telnetclient** *value* command.

Examples

This example shows how to enable client timeout.

```
Device> enable
Device# configure terminal
Device(config)# telnetclient timeout
```

Related Commands

Command	Description
telnet *server-ip*	Logins to the Telnet server

timeout

To enable the client timeout, use the **timeout** command in privileged EXEC mode. To disable the client timeout function, use the **no timeout** command.

timeout *value*

no timeout

Syntax Description

value	The system idle timeout value. The unit is minutes. The range is from 1 to 480.

Command Modes

Privileged EXEC (#)

Usage Guidelines

Use this command on the OLT configured as the Telnet server. To enable the client timeout, use the **timeout** command. To configure the client timeout value, use the **timeout** *value* command.

Examples

This example shows how to configure a client timeout interval of 30 minutes.

```
Device> enable
Device# timeout 30
```

Related Commands

Command	Description
telnet enable	Enables Telnet on a OLT and configures the OLT as the Telnet server.

translate old-vlan

To configure the VLAN translate rule, use the **translate old-vlan** command in VLAN profile configuration mode. To disable the **no translate old-vlan** command.

translate old-vlan *vlan_id* {*priority* | **new-vlan** *vlan_id* [*priority*]}

no translate old-vlan *vlan_id* [*priority*]

Syntax Description

priority	The priority value. The range is from 0 to 7.
vlan_id	The VLAN ID The range is from 1 to 4094.

Command Modes

VLAN profile configuration (deploy-profile-vlan)

Usage Guidelines

A VLAN profile type must be configured.

Modifying and activating the VLAN template will cause the ONT that references the template to go online again.

Examples

This example shows how to configure the VLAN translate rule

```
Device> enable
Device# configure terminal
Device(config)# deploy profile vlan
Device(deploy-profile-vlan)# aim 5
Device(deploy-profile-vlan-5)# translate old-vlan 2 2 new-vlan 10 5
Device(deploy-profile-vlan-5)# active
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

type 1 fix

To configure only a fixed bandwidth, use the **type 1 fix** *fixed_bandwidth* command in DBA profile configuration mode.

type 1 fix *fixed_bandwidth*

Syntax Description

fixed_bandwidth	The fixed bandwidth in kbps. The range is fro The fixed bandwidth must be divisible by 64 k

Command Modes

DBA profile configuration (deploy-profile-dba)

Usage Guidelines

Type 1 T-CONT is preferred for services that are sensitive to the data forwarding delay. For example, VoIP services.

A DBA profile type must be configured.

Modifying and activating the DBA profile will cause the ONT that references the template to go online again.

Examples

This example shows how to configure type 1 T-CONT.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile dba
Device(deploy-profile-dba)# aim 5
Device(deploy-profile-dba-5)# type 1 fix 1024
Device(deploy-profile-dba-5)# active
```

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

type 2

To configure only the assured bandwidth, use the **type 2 assured** *assured_bandwidth* command in DBA profile configuration mode.

type 2 assured *assured_bandwidth*

Syntax Description

assured_bandwidth	The assured bandwidth in kbps. The rang The assured bandwidth must be divisible

Command Modes

DBA profile configuration (deploy-profile-dba)

Usage Guidelines

Type 2 T-CONT is preferred for services without strict delay and jitter requirements. For example, IPTV multicast services.

A DBA profile type must be configured.

Modifying and activating the DBA profile will cause the ONT that references the template to go online again.

Examples

This example shows how to configure type 2 T-CONT.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile dba
Device(deploy-profile-dba)# aim 5
Device(deploy-profile-dba-5)# type 2 assured 1024
Device(deploy-profile-dba-5)# active
```

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

type 3

To configure both assured bandwidth and non-assured bandwidth, use the **type 3 assured** *assured_bandwidth* **max** *max_bandwidth* command in DBA profile configuration mode.

type 3 assured *assured_bandwidth* **max** *max_bandwidth*

Syntax Description

assured_bandwidth	The assured bandwidth in kbps. The range is The assured bandwidth must be divisible by
max_bandwidth	The maximum bandwidth in kbps. The range The maximum bandwidth must be divisible

Command Modes

DBA profile configuration (deploy-profile-dba)

Usage Guidelines

Type 3 T-CONT is preferred for services with variable-rate burst traffic.

A DBA profile type must be configured.

Modifying and activating the DBA profile will cause the ONT that references the template to go online again.

Examples

This example show how to configure both assured bandwidth and non-assured bandwidth.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile dba
Device(deploy-profile-dba)# aim 5
Device(deploy-profile-dba-5)# type 3 assured 1024 max 2500
Device(deploy-profile-dba-5)# active
```

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

type 4

To configure the optimum bandwidth, use the **type 4 max** *max_bandwidth* command in DBA profile configuration mode.

type 4 max *max_bandwidth*

Syntax Description

max_bandwidth	The maximum bandwidth in kbps. The range The maximum bandwidth must be divisible b

Command Modes

DBA profile configuration (deploy-profile-dba)

Usage Guidelines

Type 4 T-CONT is preferred for services with variable-rate burst traffic which does not exhibit delay sensitivity. For example, internet data services.

A DBA profile type must be configured.

Modifying and activating the DBA profile will cause the ONT that references the template to go online again.

Examples

This example show how to configure the optimum bandwidth.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile dba
Device(deploy-profile-dba)# aim 5
Device(deploy-profile-dba-5)# type 4 max 1024
Device(deploy-profile-dba-5)# active
```

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

type 5

To configure a combination of fixed, assured and best-effort bandwidth, use the **type 5 fix** *fixed_bandwidth* **assured** *assured_bandwidth* **max** *max_bandwidth* command in DBA profile configuration mode.

type 5 fix *fixed_bandwidth* **assured** *assured_bandwidth* **max** *max_bandwidth*

Syntax Description

fixed_bandwidth	The fixed bandwidth in kbps. The range The fixed bandwidth must be divisible b
assured_bandwidth	The assured bandwidth in kbps. The ran The assured bandwidth must be divisible
max_bandwidth	The maximum bandwidth in kbps. The r The maximum bandwidth must be divis kbps.

Command Modes

DBA profile configuration (deploy-profile-dba)

Usage Guidelines

Type 5 T-CONT is preferred for services with general traffic.

A DBA profile type must be configured.

Modifying and activating the DBA profile will cause the ONT that references the template to go online again.

Examples

This example show how to configure a combination of fixed, assured and best-effort bandwidth

```
Device> enable
Device# configure terminal
Device(config)# deploy profile dba
Device(deploy-profile-dba)# aim 5
Device(deploy-profile-dba-5)# type 5 fix 1024 assured 1024 max 2048
Device(deploy-profile-dba-5)# active
```

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

upload keyfile

To upload the local key to the key server, use the **upload keyfile** command in privileged EXEC mode.

Upload to a TFTP server

upload keyfile {**public** | **private**} **tftp** {**inet** | **inet6**} *server_ip filename*

Upload to a FTP server

upload keyfile {**public** | **private**} **ftp** {**inet** | **inet6**}*server_ip filename*

Syntax Description

public	The public SSH key file
private	The private SSH key file
tftp	Loads the file from the TFTP server.
ftp	Loads the file from FTP server.
inet	The IPv4 address family.
inet6	The IPv6 address family
server_ip	The server IP address
filename	The key filena,e.

Command Modes

Privileged EXEC (#)

Usage Guidelines

SSH must be enabled on the device.

Examples

This example shows how to upload the local key to the FTP server

```
Device> enable
Device# upload keyfile public ftp inet 100.100.100.1 mykey  admin 123456
```

Related Commands

Command	Description
ssh	Enables SSH on an OLT.
load keyfile	Downloads the key from the external key server

us car

To configures GEM port traffic control, use the **us car cir** *cir* **cbs** *cbs* **pir** *pir* **pbs** *pbs* command in uplink traffic profile configuration mode.

us car cir *cir* **cbs** *cbs* **pir** *pir* **pbs** *pbs*

Syntax Description

cir *cir*	The committed information rate in k The range is from 64 to 800000
cbs *cbs*	The committed burst size in KB. The range is from 2 to 25000.
pir *pir*	The peak information rate in kbps. The range is from 64 to 1024000.
pbs *pbs*	The peak burst size in KB. The range is from 2 to 25000.

Command Modes

Uplink traffic profile (deploy-profile-us-traffic)

Usage Guidelines

An uplink profile type must be configured.

The peak information rate requirement is greater than or equal to committed information rate.

Modifying and activating the uplink traffic profile will cause the ONT that references the template to go online again.

Examples

This example shows how to configures GEM port traffic control.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile us-traffic
Device(deploy-profile-us-traffic)# aim 5
Device(deploy-profile-us-traffic-5)# us queue 1
Device(deploy-profile-us-traffic-5)# us car cir 128 cbs 1024 pir 128 pbs 24
Device(deploy-profile-us-traffic-5)# active
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

us queue

To configure GEM port queue priority, use the **us queue** command in uplink traffic profile configuration mode.

us queue *priority_queue*

Syntax Description

priority_queue	The priority queue. The range is from 0 to 7.

Command Modes

Uplink traffic profile (deploy-profile-us-traffic)

Usage Guidelines

An uplink profile type must be configured.

Examples

This example shows how to configure GEM port queue priority

```
Device> enable
Device# configure terminal
Device(config)# deploy profile us-traffic
Device(deploy-profile-us-traffic)# aim 5
Device(deploy-profile-us-traffic-5)# us queue 1
```

Related Commands

Command	Description
deploy profile	Deploys a profile type
aim	Creates aim based on the profile.

us queue

PART II

Managing Users

Managing Users

aaa

To enter Authentication Authorization and Accounting (AAA) configuration mode, use the **aaa** command in global configuration mode.

aaa

Command Modes

Global configuration (config)

Examples

This example shows how to enter AAA configuration mode.

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)#
```

Related Commands

Command	Description
auth-secret-key	Configures a RADIUS authentication key
default domain-name	Enables or disables the default domain
domain *domain_name*	Specifies a RADIUS domain name

auth-secret-key

To configure a RADIUS authentication key, use the **auth-secret-key** command in AAA configuration mode. To delete the configured RADIUS authentication key, use the **no** form of the command.

auth-secret-key *key*
no auth-secret-key

Syntax Description

key	The secret key.

Command Modes

AAA configuration (config-aaa)

Usage Guidelines

Use this command in the AAA configuration mode.

Examples

This example shows how to configure a RADIUS authentication key

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius host radius1
Device(config-aaa-radius-radius1)# auth-secret-key key1
```

Related Commands

Command	Description
aaa	Enters AAA configuration mode

default domain-name

To enable or disable the default domain, use the **default domain-name** command in AAA configuration mode.

default domain-name {**enable** *domain-name* | **disable**}

Syntax Description

enable	Enables the default domain.
domain-name	The default domain name The format is string.
disable	Disables the default domain.

Command Modes

AAA configuration (config-aaa)

Usage Guidelines

Use this command in the AAA configuration mode.

Examples

This example shows how to configure the default domain.

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# domain default1
Device(config-aaa-domain-default1)# radius host binding cisco
Device(config-aaa-domain-default1)# state active
Device(config-aaa-domain-default1)# exit
Device(config-aaa)# default domain-name enable domain1
 Succeed in setting default domain.
```

Related Commands

Command	Description
aaa	Enters AAA configuration mode

domain

To specify a RADIUS domain name, use the **domain** *domain_name* command in AAA configuration mode.

domain *domain_name*

Syntax Description

domain_name	The name of the domain. The format is string.

Command Modes

AAA configuration (config-aaa)

Usage Guidelines

Use this command in the AAA configuration mode.

Examples

This example shows how to specify the RADIUS domain name

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# domain domain1
Device(config-aaa-domain-domain1)#
```

Related Commands

Command	Description
aaa	Enters AAA configuration mode

login-access-list

To allow access for specific IP addresses, use the **login-access-list** {**snmp** | **ssh** | **telnet**} command in global configuration mode. To block all IP addresses, use the **no login-access-list** command.

login-access-list {**snmp** *ip_address mask* | **ssh** *ip_address mask* | **telnet** *ip_address mask* | **telnet-limit** *max_user_number*}

no login-access-list {**snmp** {**all** | *ip_address mask*} | **ssh** {**all** | *ip_address mask*} | **telnet** {**all** | *ip_address mask*} | **telnet-limit** *max_user_number*}

Syntax Description

snmp	The SNMP
ssh	The SSH cli
telnet	The Telnet c
all	Deletes all I
ip_address	The IP addr
mask	The IP addr
telnet-limit *max_user_number*	Limit the nu The range is

Command Modes

Global configuration (config)

Usage Guidelines

Use the **no login-access-list** {**snmp**| **ssh** |**telnet**}**all** command to block all IP access.

Use the **login-access-list** {**snmp**| **ssh** |**telnet**} **0.0.0.0** [**0.0.0.0** | **255.255.255.255**] command to allow all IP access.

Examples

This example shows how to delete all IP addresses from the SNMP client.

```
Device> enable
Device# configure terminal
Device(config)# no login-access-list snmp all
Delete access ip address successfully.
```

Related Commands

Command	Description
show login-access-list	Displays the list of allowed IP addresses.

muser local

To enable local authentication mode, use the **muser local** command in global configuration mode.

muser local

Command Modes

Global configuration (config)

Examples

This example shows how to enable local authentication mode

```
Device> enable
Device# configure terminal
Device(config)# muser local
Config manager user authentication successfully.
```

Related Commands

Command	Description
show muser	Displays the authentication configuration

muser radius

To enable RADIUS remote authentication, use the **muser radius** *radius_name* command in global configuration mode.

muser radius *radius_name* {**pap** | **chap**} {**account** | **local**}

Syntax Description

radius_name	The RADIUS host name. The format is string. The range is from 1 to 32
pap	The password authentication protocol (PAP)
chap	The challenge handshake authentication proto
account	Manages login accounting through the RADIU
local	Allows local authentication when the remote a

Command Modes

Global configuration (config)

Examples

This example shows how to enable RADIUS remote authentication.

```
Device> enable
Device# configure terminal
Device(config)# muser radius cisco pap local
```

Related Commands

Command	Description
show muser	Displays the authentication configuration

muser tacacs+

To enable TACACS+ remote authentication mode, use the **muser tacacs+** command in global configuration mode.

muser tacacs+ {**author** | **account** | **command-account** | **local**}

Syntax Description

author	Allows login authorization through the TACACS+ server
account	Manages login accounting through the TACACS+ server.
command-account	Forwards all the command lines to the TACACS+ server th
local	Allows local authentication when the remote authenticatio

Command Modes

Global configuration (config)

Examples

This example shows how to enable TACACS+ remote authentication.

```
Device> enable
Device# configure terminal
Device(config)# muser tacacs+
```

Related Commands

Command	Description
show muser	Displays the authentication configuration

radius host

To configure a RADIUS server name, use the **radius host** command in AAA configuration mode.

radius host *radius_name*

Syntax Description

radius_name	The name of the RADIUS serve

Command Modes

AAA configuration (config-aaa)

Usage Guidelines

Use this command in the AAA configuration mode.

Examples

This example shows how to configure a RADIUS server name

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius host radius1
```

Related Commands

Command	Description
aaa	Enters AAA configuration mode
show radius host	Displays the RADIUS host configuration

radius host binding

To bind a domain to the RADIUS server name, use the **radius host binding** command in AAA configuraton mode.

radius host binding *radius-name*

Syntax Description

radius-name	The RADIUS name server. The format is string.

Command Modes

AAA configuration (config-aaa)

Usage Guidelines

Use this command in the AAA configuration mode.

Examples

This example shows how to bind the RADIUS host to the domain.

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# domain radius1
Device(config-aaa-domain-radius1)# radius host binding cisco
```

Related Commands

Command	Description
aaa	Enters AAA configuration mode
show radius host	Displays the RADIUS host configuration

service password-encryption

To save a password in cipher text, use the **service password-encryption** command in global configuration mode.

service password-encryption

Command Modes

Global configuration (config)

Examples

This example shows how to save a password in cipher text

```
Device> enable
Device# configure terminal
Device(config)# service password-encryption
```

show domain

To display the domain configuration, use the **show domain** command in privileged EXEC or global configuration mode.

show domain [*domain_name*]

Syntax Description

domain_name	The name of the domain. The format is string.

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to display the domain configuration.

```
Device> enable
Device# configure terminal
Device(config)# show domain domain1
 Default domain name : domain1
 DomainName       : domain1
 RADIUSServerName : cisco
 Access-limit     : disabled
 AccessedNum      : 0
 Scheme           : radius
 State            : Block
------------------------------------------------------------------------

 Total [1] item(s).
```

show login-access-list

To display the list of allowed IP addresses, use the **show login-access-list** command in privileged EXEC or global configuration mode.

show login-access-list

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the list of allowed IP addresses.

```
Device> enable
Device# configure terminal
Device(config)# show login-access-list
sno  ipAddress  wildcard bits    terminal
1    0.0.0.0    255.255.255.255  telnet
2    0.0.0.0    255.255.255.255  ssh
```

Related Commands

Command	Description
login-access-list {**snmp** | **ssh** | **telnet**}	Allows access for specific IP addresses

show muser

To display the authentication configuration, use the **show muser** command in privileged EXEC or global configuration mode.

show muser

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the authentication configuration.

```
Device> enable
Device# configure terminal
Device(config)# show muser
Show manager user authentication.
Authentication type : local
Admin-Remote-Auth: Disable
```

show running-config oam

To display the timeout configuration, use the **show running-config oam** command in privileged EXEC or global configuration mode.

show running-config oam

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the timeout configuration.

```
Device> enable
Device# configure terminal
Device(config)# show running-config oam
![OAM]
no login-access-list snmp 0.0.0.0 255.255.255.255
service password-encryption
username text privilege 0 password 7 884863d2
banner
screen-rows per-page 55
hostname 2
telnet limit 3
exit
timeout 100
configure terminal
telnetclient timeout 2
ip icmp mask-reply
```

show tacacs+

To display the TACACS+ configuration, use the **show tacacs+** command in privileged EXEC or global configuration mode.

show tacacs+

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the TACACS+ configuration.

```
Device> enable
Device# configure terminal
Device(config)# show tacacs+
Primary Server Configurations:
IP address: : 192.168.1.10
Connection port: : 49
Connection timeout: : 5
Key: : 123456

Secondary Server Configurations:
IP address: : 192.168.1.11
Connection port: : 49
Connection timeout: : 5
Key: : 123456
```

show username

To display the user information, use the **show username** command in privileged EXEC or global configuration mode.

show username *username*

Syntax Description

username	The user name.

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the user information.

```
Device> enable
Device# configure terminal
Device(config)# show username admin
display user information
Terminal type: C=Console, T=Telnet, S=SSH, W=Web
Global Failmax: n/a
User Name         Role     Terminal  FailMax   Fail      OnLineMax  OnLine
_____________________________________________________________________________
admin             ADMIN    CTSW      n/a       0         n/a        1
```

Related Commands

Command	Description
username *username*	Adds a user

show username privilege-auth

To display the privilege password authentication configuration, use the **show username privilege-auth** command in privileged EXEC or global configuration mode.

show username privilege-auth

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the configuration of second-tier password authentication

```
Device> enable
Device# configure terminal
Device(config)# show username privilege-auth
Privilege-password authentication
  switch: OFF
  remote-user name: remote_admin
  password not configured
```

Related Commands

Command	Description
username privilege-auth	Enables privilege password authentication for a local user

show username silent

To display a user silent period information, use the **show username silent** command in privileged EXEC or global configuration mode.

show username silent

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view a user silent period information

```
Device> enable
Device# configure terminal
Device(config)# show username silent
display user silent period information
Silent Time: 2 minutes
User Name         State     Silent End Time

_____________________________________________
admin             Off       n/a
text              Off       n/a
```

Related Commands

Command	Description
username *username*	Adds a user
username silent-time	Configures the silent time
show username	Displays the user information

show users

To display the online users, use the **show users** command in privileged EXEC or global configuration mode.

show users

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the online users.

```
Device> enable
Device# configure terminal
Device(config)# show users
Only 5 users logged in by telnet are allowed to be in privileged mode.
Now 1 users logged in by telnet have been in privileged mode.

User "admin" logged in at time 2001/12/09 16:53:44
Time passed after login: 0 days 0 hours 12 minutes 32 seconds
Time no operation: 0 minutes 0 seconds
Terminal: telnet 1
Transport: telnet
User's IP address: 10.65.75.54
Authentication: local
Radius hostname: N/A
```

state active

To activate a domain, use the **state active** command in AAA configuration mode.

state active

Command Modes

AAA configuration (config-aaa)

Examples

This example shows to activate a configured domain.

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# domain default1
Device(config-aaa-domain-default1)# radius host binding cisco
Device(config-aaa-domain-default1)# state active
Device(config-aaa-domain-default1)# exit
```

Related Commands

Command	Description
state block	Deactivates a domain

state block

To deactivate a domain, use the **state block** command in AAA configuration mode.

state block

Command Modes

AAA configuration mode

Examples

This example shows how to deactivate a domain.

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# domain default1
Device(config-aaa-domain-default1)# state block
```

Related Commands

Command	Description
state active	Activates a domain

stop

To force user or users to go offline, use the **stop** command in privileged EXEC mode.

stop {*username* | **vty** {**all** *vty_list*} | **telnet** {**all** *terminal_id*}}

Syntax Description

username	The username
all	Stops all.
vty_list	The VTY list.
terminal_id	The terminal ID The range is from 0 to 5.

Command Modes

Privileged EXEC (#)

Examples

This example shows how to force a user offline

```
Device> enable
Device# stop Jerry
```

tacacs+

To configure the TACACS + server, use the **tacacs+** command in global configuration mode.

tacacs+ {**primary** | **secondary**}**server** *ip_address* [**encrypt-key** *value* | **key** *key* | **port** *port* | **timeout** *value*]

Syntax Description

primary	Configures the primary server.
secondary	Configures the secondary server
server *ip_address*	The server IP address.
encrypt-key *value*	The server key encryption.
key *key*	The server key configuration.
port*port*	The TCP port. The range is from 1 to 65535.
timeout *value*	The connection timeout. The range is from 1 to 70. The d

Command Modes

Global configuration (config)

Examples

This example shows how to configure the TACACS + primary server

```
Device> enable
Device# configure terminal
Device(config)# tacacs+ primary server 192.168.1.10 key 123456
```

Related Commands

Command	Description
show tacacs+	Displays the TACACS+ configuration

tacacs+ authentication-type

To configure an authentication type, use the **tacacs+ authentication-type** command in global configuration mode.

tacacs+ authentication-type {**ascii** | **chap** | **pap**}

Syntax Description

ascii	Configures the ASCII authentication type.
chap	Configures the Challenge Handshake Authentication Protoc
pap	Configures the Password Authentication Protocol (PAP) au

Command Modes

Global configuration (config)

Examples

This example shows how to configure an ASCII authentication type

```
Device> enable
Device# configure terminal
Device(config)# tacacs+ authentication-type ascii
```

Related Commands

Command	Description
show tacacs+	Displays the TACACS+ configuration

tacacs+ encrypt-key

To enable password encryption, use the **tacacs+ encrypt-key** command in global configuration mode. To disable password encryption, use the **no tacacs+ encrypt-key** command.

tacacs+ encrypt-key

no tacacs+ encrypt-key

Command Modes

Global configuration (config)

Examples

This example shows how to enable password encryption

```
Device> enable
Device# configure terminal
Device(config)# tacacs+ encrypt-key
```

Related Commands

Command	Description
show tacacs+	Displays the TACACS+ configuration

tacacs+ preemption-time

To configure the recovery time to switch to the TACACS+ primary server, use the **tacacs+ preemption-time** command in global configuration mode.

tacacs+ preemption-time *time*

Syntax Description

time	The preemption time The unit in minutes. The range is from 0 to 1440. The default value isc0

Command Modes

Global configuration (config)

Examples

This example shows how to configure the recovery time to switch to the TACACS+ primary server.

```
Device> enable
Device# configure terminal
Device(config)# tacacs+ preemption-time 200
```

Related Commands

Command	Description
show tacacs+	Displays the TACACS+ configuration

timeout

To configure the system idle timeout, use the **timeout** command in privileged Exec mode. To disable the system idle timeout, use the **no timeout** command.

timeout *value*

no timeout

Syntax Description

value	The system idle timeout value. The range is 1-480. The default timeout value is 20m.

Command Modes

Privileged Exec (#)

Examples

This example shows how to configure the system idle timeout

```
Device> enable
Device# timeout 100
The idle time is : 100 minutes!
```

username

To add a user or modify an existing user privilege level, use the **username** *username* command in global configuration mode. To remove a user, use the **no username** *username* command.

username *username* {**password** {**0** | **7**}*password* | **privilege** *privilege_level* **password** {**0** | **7**}*password* | **terminal** {**all** | **console** | **none** | **ssh** | **telnet** | **web**}}

no username *username*

Syntax Description

username	The username.
password 0 |7	The password encryption time. • A value of 0 means the pa • A value of 7 means the pa
password	The password.
privilege_level	The privilege level. • A privilege value of 0 or 1 • A privilege value between • Super user (admin) requir
terminal	The login mode The options are • console • none • SSH • Telnet • Web

Command Modes

Global configuration (config)

Usage Guidelines

If you do not enter a permission value when you create a user, the system will automatically assign it with normal permissions.

Configure the password encryption type as 0 for a new user. When you configure the **service password-encryption** command, a password configured in plain text (0) is decrypted in de-compilation and the decrypted password type changes to 7

Examples

This example shows how to add a new user.

```
Device> enable
Device# configure terminal
Device(config)# username mark privilege 0 password 0 mark@123
Add user successfully.
```

Related Commands

Command	Description
show username	Displays the user information
username change-password	Modifies the user password
username change-privilege-pwd	Configures the second-tier password authentication
username failmax	Configures a limit on the consecutive failed login attempts
username online-max	Configures the duration users are online at the same time
username silent-time	Configures the silent time

username change-password

To modify the user password, use the **username change-password** command in global configuration mode.

username change-password

Command Modes

Global configuration (config)

Examples

This example shows how to modify the user password

```
Device> enable
Device# configure terminal
Device(config)# username change-password
```

Related Commands

Command	Description
username *username*	Adds a user
show username	Displays the user information

username change-privilege-pwd

To configure the second-tier password authentication, use the **username change-privilege-pwd** command in global configuration mode.

username change-privilege-pwd {**0** | **7**}

Syntax Description

{ **0** |**7**}	• A value of 0 means the passwo • A value of 7 means the passwo

Command Modes

Global configuration (config)

Examples

This example shows how to configure the second-tier password authentication.

```
Device> enable
Device# configure terminal
Device(config)# username change-privilege-pwd 0 123456
```

Related Commands

Command	Description
username *username*	Adds a user
show username	Displays the user information

username failmax

To configure a limit on the consecutive failed login attempts, use the **username failmax** command in global configuration mode. To disable the limit on the consecutive failed login attempts, use the **no username failmax** command.

username failmax {*fail_value* | *username fail_value*}

no username failmax

Syntax Description

fail_value	The fail value. The range is from 1 to 100.
username	The username.

Command Modes

Global configuration (config)

Examples

This example shows how to configure a limit on the consecutive failed login attempts.

```
Device> enable
Device# configure terminal
Device(config)# username failmax 5
```

Related Commands

Command	Description
username *username*	Adds a user
show username	Displays the user information

username online-max

To configure the duration users are online at the same time, use the **username online-max** command in global configuration mode.

username online-max *username value*

Syntax Description

username	The username.
value	The duration users are online at the same time The range is from 1 to 100.

Command Modes

Global configuration (config)

Examples

This example shows how to configure the duration users are online at the same time.

```
Device> enable
Device# configure terminal
Device(config)# username online-max mark 100
```

Related Commands

Command	Description
username *username*	Adds a user
show username	Displays the user information

username privilege-auth-remote-user

To enable privilege password authentication for a remote user, use the **username privilege-auth-remote-user** command in global configuration mode. To disable user privilege password authentication, use the **no username privilege-auth** command.

username privilege-auth-remote-user *username*

no username privilege-auth-remote-user

Syntax Description

username	The username.

Command Modes

Global configuration (config)

Examples

This example shows how to enable privilege password authentication.

```
Device> enable
Device# configure terminal
Device(config)# username privilege-auth-remote-user mark
Enable Privilege-password authentication OK!
```

Related Commands

Command	Description
show username	Displays the user information

Related Commands

Command	Description
username *username*	Adds a user
show username	Displays the user information

username privilege-auth

To enable privilege password authentication for a user, use the **username privilege-auth** command in global configuration mode. To disable user privilege password authentication, use the **no username privilege-auth** command.

username privilege-auth [**always**]

no username privilege-auth

Syntax Description

always	Configures privilege password authentication for al

Command Modes

Global configuration (config)

Examples

This example shows how to enable user privilege password authentication.

```
Device> enable
Device# configure terminal
Device(config)# username privilege-auth
Enable Privilege-password authentication OK!
```

Related Commands

Command	Description
show username	Displays the user information

Related Commands

Command	Description
username *username*	Adds a user.
show username	Displays the user information.
show username privilege-auth	Displays the privilege password authentication configuration.

username silent-time

To configure the silent time, use the **username silent-time** command in global configuration mode.

username silent-time *silent_time*

Syntax Description

silent_time	The silence period time. The range is from 2 to 1440.

Command Modes

Global configuration (config)

Examples

This example shows how to configure the silent time

```
Device> enable
Device# configure terminal
Device(config)# username silent-time 100
```

Related Commands

Command	Description
show username	Displays the user information

Related Commands

Command	Description
username *username*	Adds a user
show username	Displays the user information
show username silent	Displays a user silent period information

PART III

OLT Port Configuration

OLT Port Configuration

channel-group group_id

To configure the aggregation group ID, use the **channel-group** *channel_group_id* command in global configuration mode. To disable the aggregation group ID, use the **no channel-group** *channel_group_id* command.

channel-group *channel_group_id*

no channel-group *channel_group_id*

Syntax Description

channel_group_id	The channel group ID. The range is 0-5.

Command Modes

Global configuration (config)

Examples

This example shows how to configure the aggregation group ID

```
Device> enable
Device# configure terminal
Device(config)# channel-group 4
```

channel-group load-balance

To configure a load balance policy, use the **channel-group load-balance** command in global configuration mode. To disable a load balance policy, use the **no channel-group load-balance** form of this command.

channel-group load-balance {**dst-ip** | **dst-mac** | **src-dst-ip** | **src-dst-mac** | **src-ip** | **src-mac**}

no channel-group load-balance

Syntax Description

dst-ip	Configures the load balance policy based on desti
dst-mac	Configures the load balance policy based on desti
src-dst-ip	Configures the load balance policy based on sour
src-dst-mac	Configures the load balance policy based on sour
src-ip	Configures the load balance policy based on sour
src-mac	Configures the load balance policy based on sour

Command Modes

Global configuration (config)

Examples

This example shows how to configure a load balance policy based on source MAC.

```
Device> enable
Device# configure terminal
Device(config)# channel-group load-balance src-mac
```

channel-group group_id mode

To add a port to an aggregation group, use the **channel-group** *channel_group_id* **mode** command in interface configuration mode. To disable the aggregation group ID, use the **no channel-group** *channel_group_id* **mode** command.

channel-group *channel_group_id* **mode** {**on** | **active** | **passive**}

no channel-group *channel_group_id* **mode**

Syntax Description

channel_group_id	The channel group ID. The range is 0-5.
on	Configures the LACP static mode.
active	Configures the LACP active mode
passive	Configures the LACP passive mode

Command Modes

Interface configuration (config-if)

Examples

This example shows how to add a port to an aggregation group.

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/1
Device(config-if-ethernet-1/1)# channel-group 2 mode active
```

clear channel-group

To clear the LACP statistical information, use the **clear channel-group** *channel_group_id* command in global configuration mode.

clear channel-group [*channel_group_id*]

Syntax Description

channel_group_id	The channel group ID. The range is 0-5.

Command Modes

Global configuration (config)

Examples

This example shows how to clear the LACP statistical information.

```
Device> enable
Device# configure terminal
Device(config)# clear channel-group
Clear channel group statistics information record successfully.
```

clear interface

To clear interface statistics information, use the **clear interface** command in global configuration mode.

clear interface {*slot-number* | **ethernet** *slot-number/port-number* | **gpon** *slot-number/port-number* }

Syntax Description

slot-number	The slot number. The range is from 0 to 3.
slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1. • 10GE Ethernet: The value is 2. • *port-number*: • GPON: The range is from 1 to • GE Ethernet: The range is from • 10GE Ethernet: The range is fr

Command Modes

Global configuration (config)

Examples

This example shows how to clear interface statistics information

```
Device> enable
Device# configure terminal
Device(config)# clear interface ethernet 0/1
clear ports statistics information record successfully.
```

interface range ethernet

To configure port mode in bulk, use the **interface range ethernet** command in interface configuration mode.

interface range ethernet *slot-number/port-number* **to ethernet** *slot-number/port-number*

Syntax Description

slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1 • 10GE Ethernet: The value i • *port-number*: • GPON: The range is from 1 • GE Ethernet: The range is f • 10GE Ethernet: The range i

Command Modes

Interface configuration (config-if)

Examples

This example shows how to configure port mode in bulk

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/1
Device(config-if-ethernet-1/1)# interface range ethernet 1/1 to ethernet 1/4
Device(config-if-range)#
```

lacp port-priority

To configure port priority, use the **lacp port-priority** command in interface configuration mode. To disable port priority, use the **no lacp port-priority** command.

lacp port-priority *priority_value*

no lacp port-priority

Syntax Description

priority_value	The priority value. The range is from 1 to 65535.

Command Modes

Interface configuration (config-if)

Examples

This example shows how to configure port priority.

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/1
Device(config-if-ethernet-1/1)# lacp port-priority 8
```

lacp system-priority

To configure system priority, use the **lacp system-priority** command in global configuration mode. To disable port priority, use the **no lacp system-priority** command.

lacp system-priority *priority_value*

no lacp system-priority

Syntax Description

priority_value	The priority value. The range is from 1 to 65535.

Command Modes

Global configuration (config)

Examples

This example shows how to configure the system priority.

```
Device> enable
Device# configure terminal
Device(config)# lacp system-priority 3
```

port-control mode primary

To configure the primary mode, use the **port-control mode primary** command in interface configuration mode. To disable the primary mode, use the **no port-control mode** command.

port-control mode primary
no port-control mode

Command Modes

Interface configuration (config-if)

Examples

This example shows how to configure the primary mode.

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/1
Device(config-if-ethernet-1/1)# port-control mode primary
```

port-control mode secondary

To configure the secondary mode, use the **port-control mode secondary** command in interface configuration mode. To disable the secondary mode, use the **no port-control mode** command.

port-control mode secondary
no port-control mode

Command Modes

Interface configuration (config-if)

Examples

This example shows how to configure the secondary mode.

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/1
Device(config-if-ethernet-1/1)# port-control mode secondary
```

port-isolation

To configure port isolation, use the **port-isolation** command in global configuration mode. To disable port isolation, use the **no port-isolation** command.

port-isolation ethernet *slot-number/port-number*

no port-isolation ethernet *slot-number/port-number*

Syntax Description

slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1. • 10GE Ethernet: The value is 2. • *port-number*: • GPON: The range is from 1 to • GE Ethernet: The range is from • 10GE Ethernet: The range is fr

Command Modes

Global configuration (config)

Examples

This example shows how to configure port isolation.

```
Device> enable
Device# configure terminal
Device(config)# port-isolation ethernet 1/1
Add port isolation downlink port successfully.
```

Related Commands

Command	Description
show port-isolation	Displays the isolation port

port-rate-statistics interval

To configure port interface statistic interval, use the **port-rate-statistics interval** *value* command in global configuration mode. To restore the default value, use the **no** form of this command.

port-rate-statistics interval *value*

no port-rate-statistics interval

Syntax Description

value	The time interval range. The range is from 1 to 5. The unit is minutes. The d

Command Modes

Global configuration (config)

Examples

This example shows how to configure port interface statistic interval.

```
Device> enable
Device# configure terminal
Device(config)# port-rate-statistics interval 3
Port rate statistics interval has been changed, and will
restart calculating port average rate!
```

psg group-id force-switch

To force a port changeover, use the **psg** *group-id* **force-switch** command in global configuration mode

psg *group-id* **force-switch**

Syntax Description

group-id	The protection switch group ID. The range is 0 to 7.

Command Modes

Global configuration (config)

Examples

This example shows how to force a switch changeover.

```
Device> enable
Device# configure terminal
Device(config)# psg 1 type-b primary interface gpon 0/3 secondary interface gpon 0/1
Config success.
Device(config)# psg 1 force-switch
Switch success.
```

psg group-id type-b

To configure a protection switch group, use the **psg** *group-id* **type-b primary interface gpon** *slot-number/port-number* **secondary interface gpon** *slot-number/port-number* command in global configuration mode. To remove the protection switch group, use the **no psg** *group-id* command.

psg *group-id* **type-b primary interface gpon** *slot-number/port-number* **secondary interface gpon** *slot-number/port-number*
no psg *group-id*

Syntax Description

group-id	The protection switch group ID. The range is from 0 to 7.
slot-number/port-number	• *slot-number*: The GPON slot number. The value is 0. • *port-number*: The GPON port number. The range is from 1 to 8.

Command Modes

Global configuration (config)

Examples

This example shows how to configure a protection switch group.

```
Device> enable
Device# configure terminal
Device(config)# psg 1 type-b primary interface gpon 0/3 secondary interface gpon 0/1
Config success.
```

show description

To display the interface description, use the **show description** command in privileged EXEC or global configuration mode.

show description interface ethernet *slot-number/port-number*

Syntax Description

slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1. • 10GE Ethernet: The value is 2. • *port-number*: • GPON: The range is from 1 to • GE Ethernet: The range is from • 10GE Ethernet: The range is fr

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the interface description.

```
Device> enable
Device# configure terminal
Device(config)# show description interface ethernet 1/1
Port     description
e1/1     text
Total entries: 1.
```

show interface sfp

To display information about SFP parameters, use the **show interface sfp** command in privileged EXEC or global configuration mode.

show interface sfp {**ethernet** | **gpon** }*slot-number/port-number*

Syntax Description

slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1 • 10GE Ethernet: The value i • *port-number*: • GPON: The range is from 1 • GE Ethernet: The range is f • 10GE Ethernet: The range i

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the information about SFP parameters

```
Device> enable
Device# configure terminal
Device(config)# show interface sfp ethernet 1/1
```

show lacp internal

To display information of the aggregation group, use the **show lacp internal** command in privileged EXEC or global configuration mode.

show lacp internal [*channel_group_id*]

Syntax Description

channel_group_id	The channel group ID. The range is from 0 to 5.

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view information about the aggregation group.

```
Device> enable
Device# configure terminal
Device(config)# show lacp internal
Load balance: dst-ip

Channel: 2, static channel
Port   State   A-Key  O-Key  Priority   Logic-port   Actor-state
e1/1   down    -      -      -          9            -

Channel: 4, dynamic channel
Port   State   A-Key  O-Key  Priority   Logic-port   Actor-state

actor-state: activity/timeout/aggregation/synchronization
             collecting/distributing/defaulted/expired
```

show lacp neighbor

To display the neighbor information of the aggregation group, use the **show lacp neighbor** command in privileged EXEC or global configuration mode.

show lacp neighbor [*channel_group_id*]

Syntax Description

channel_group_id	The channel group ID. The range is from 0 to 5.

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the neighbor information of the aggregation group

```
Device> enable
Device# configure terminal
Device(config)# show lacp neighbor

Channel: 4
Local  Port   Key   Pri    ID          Timeout    Nei-state

nei-state: activity/timeout/aggregation/synchronization
           collecting/distributing/defaulted/expired
```

show lacp sys-id

To display the system priority configuration, use the **show lacp sys-id** command in privileged EXEC or global configuration mode.

show lacp sys-id

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the system priority configuration.

```
Device> enable
Device# configure terminal
Device(config)# show lacp sys-id

3,000a5a9b1815
```

show port-control mode

To display the configured port-control mode, use the **show port-control mode** command in privileged EXEC or global configuration mode.

show port-control mode

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the configured port-control mode.

```
Device> enable
Device# configure terminal
Device(config)# show port-control mode
port   negotiate-flag  port-control-mode
e1/1   enable          auto
e1/2   enable          auto
e1/3   enable          auto
e1/4   enable          auto
```

show port-isolation

To display the isolation port, use the **show port-isolation** command in privileged EXEC or global configuration mode.

show port-isolation

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view isolation port configuration.

```
Device> enable
Device# configure terminal
Device(config)# show port-isolation
Port isolation downlink port :
e1/2-e1/4.
```

Related Commands

Command	Description
port-isolation	Configures port isolation

show psg

To display the protection switch group configurations, use the **show psg** *group-id* command in privileged EXEC or global configuration mode.

show psg { *group-id* | **all** }

Syntax Description

group-id	The protection switch group ID. The range is from 0 to 7.
all	All protection switch groups

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to configure a protection switch group.

```
Device> enable
Device# configure terminal
Device(config)# show psg 0
GroupID   Member  Role      State
0         0/1     PRIMARY   WORKING
          0/2     SECONDARY STANDBY
Total: 1.
```

show statistics interface ethernet

To display the port rate statistics information, use the **show statistics interface** command in privileged EXEC or global configuration mode.

show statistics interface ethernet *slot-number/port-number*

Syntax Description

slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1. • 10GE Ethernet: The value is 2. • *port-number*: • GPON: The range is from 1 to • GE Ethernet: The range is from • 10GE Ethernet: The range is fr

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the port rate statistics information.

```
evice> enable
Device# configure terminal
Device(config)# show statistics interface ethernet 1/3
Port number  :  e1/3
last 5 minutes input rate 24784 bits/sec, 37 packets/sec
last 5 minutes output rate 1120 bits/sec, 1 packets/sec
64 byte packets:455394067
65-127 byte packets:302514090
128-255 byte packets:17535520
256-511 byte packets:20599116
512-1023 byte packets:4737262
1024-1518 byte packets:475868
788888610 packets input, 69778227468 bytes , 312945536 discarded packets
18800297 unicasts, 270957185 multicasts, 499131128 broadcasts
0 input errors, 0 FCS error, 0 symbol error, 0 false carrier
0 runts, 0 giants
12367313 packets output, 1245119790 bytes, 256 discarded packets
8303627 unicasts, 3620977 multicasts, 442709 broadcasts
0 output errors, 0 deferred, 0 collisions
0 late collisions
Total entries: 1.
```

show statistics

To display port rate statistics information, use the **show statistics interface ethernet** command in privileged EXEC or global configuration mode.

show statistics interface ethernet *slot-number/port-number*

Syntax Description

slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1 • 10GE Ethernet: The value i • *port-number*: • GPON: The range is from 1 • GE Ethernet: The range is f • 10GE Ethernet: The range i

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example show how to view the port rate statistics information.

```
Device> enable
Device# configure terminal
Device(config)# show statistics interface ethernet 1/1
Port number  :  e1/1
last 5 minutes input rate 0 bits/sec, 0 packets/sec
last 5 minutes output rate 0 bits/sec, 0 packets/sec
64 byte packets:0
65-127 byte packets:0
128-255 byte packets:0
256-511 byte packets:0
512-1023 byte packets:0
1024-1518 byte packets:0
0 packets input, 0 bytes , 0 discarded packets
0 unicasts, 0 multicasts, 0 broadcasts
0 input errors, 0 FCS error, 0 symbol error, 0 false carrier
0 runts, 0 giants
0 packets output, 0 bytes, 0 discarded packets
0 unicasts, 0 multicasts, 0 broadcasts
0 output errors, 0 deferred, 0 collisions
0 late collisions
Total entries: 1.
```

show statistics channel-group

To display LACP statistical information, use the **show statistics channel-group** command in privileged EXEC or global configuration mode.

show statistics channel-group [*channel_group_id*]

Syntax Description

channel_group_id	The channel group ID. The range is from 0 to 5.

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the LACP statistical information

```
Device> enable
Device# configure terminal
Device(config)# show statistics channel-group
Channel group : 2
last 5 minutes input rate 0 bits/sec, 0 packets/sec
last 5 minutes output rate 0 bits/sec, 0 packets/sec
64 byte packets:0
65-127 byte packets:0
128-255 byte packets:0
256-511 byte packets:0
512-1023 byte packets:0
1024-1518 byte packets:0
0 packets input, 0 bytes , 0 discarded packets
0 unicasts, 0 multicasts, 0 broadcasts
0 input errors, 0 FCS error, 0 symbol error, 0 false carrier
0 runts, 0 giants
0 packets output, 0 bytes, 0 discarded packets
0 unicasts, 0 multicasts, 0 broadcasts
0 output errors, 0 deferred, 0 collisions
0 late collisions

Channel group : 4

This channel group does not include any ports!


Total entries: 2.
```

show statistics dynamic interface

To display the real-time statistic information of an interface, use the **show statistics dynamic interface** command in privileged EXEC or global configuration mode.

show statistics dynamic interface

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the real-time statistic information of an interface.

```
Device> enable
Device# configure terminal
Device(config)# show statistics dynamic interface
Port Statistics        Sun Dec 9 17:40:29 2001
port  link   Tx Pkt    Tx Byte     Rx Pkt    Rx Byte     Rx        Rx
      Status Count     Count       Count     Count       Bcast     Mcast
================================================================================
g0/1    up   1427776E3 122120178E3 3230173   579417376   279481    171727
g0/2    down 0         0           0         0           0         0
g0/3    down 0         0           0         0           0         0
g0/4    down 0         0           0         0           0         0
g0/5    down 0         0           0         0           0         0
g0/6    down 0         0           0         0           0         0
g0/7    down 0         0           0         0           0         0
g0/8    down 0         0           0         0           0         0
e1/1    down 0         0           0         0           0         0
e1/2    down 0         0           0         0           0         0
e1/3    up   12366419  1245034896  788871832 69776674248 499122592 270949818
e1/4    down 2         210         4         256         0         4
e2/1    down 0         0           0         0           0         0
e2/2    down 0         0           0         0           0         0
==============0->Clear Counters U->page up D->page down CR->exit==============

Notes:If you see a E number, you can use the command "line width" to get more
information.
```

show utilization interface

To display the interface utilization, use the **show utilization interface** command in privileged EXEC or global configuration mode.

show utilization interface

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the interface utilization.

```
Device> enable
Device# configure terminal
Device(config)# show utilization interface
Link Utilization Averages           Tue Dec 4 19:06:53 2001
port  link    Receive   Peak Rx   Transmit  Peak Tx
      Status  pkts/sec  pkts/sec  pkts/sec  pkts/sec
================================================================
g0/1  up      0         0         16        16
g0/2  down    0         0         0         0
g0/3  down    0         0         0         0
g0/4  down    0         0         0         0
g0/5  down    0         0         0         0
g0/6  down    0         0         0         0
g0/7  down    0         0         0         0
g0/8  down    0         0         0         0
e1/1  down    0         0         0         0
e1/2  down    0         0         0         0
e1/3  up      37        37        2         2
e1/4  down    0         0         0         0
e2/1  down    0         0         0         0
e2/2  down    0         0         0         0
=====spacebar->toggle screen U->page up D->page down CR->exit=====
```

speed

To configure the interface speed, use the **speed** command in interface configuration mode. To disable the interface speed, use the **no speed** command.

speed {**1000** | **10000** | **auto**}

no speed

Syntax Description

1000	Port speed is 1000Mbps
10000	Port speed is 10000Mbps
auto	Port speed is automatic

Command Modes

Interface configuration (config-if)

Examples

This example shows how to configure the interface speed

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/1
Device(config-if-ethernet-1/1)# speed 1000
```

PART IV

VLAN Configuration

VLAN Configuration

description

To add a VLAN name or a description for the VLAN use the **description** command in the VLAN configuration mode.

description *string*

Syntax Description

string	Specifies a name or a description for the VLAN. The range is 1-32 characters.

Command Default

None

Command Modes

VLAN Configuration

Examples

```
Device(config)# vlan 11
Device(config-if-vlan)# switchport ethernet 1/3
Device(config-if-vlan)# description "vlan1"
```

ingress acceptable-frame

To configure the type of frames or VLAN packtes that are acceptable on the port, use the ingress acceptable-frame command in the Interface configuration mode.

ingress acceptable-frame {**all** | **tagged**}

Syntax Description

all	Allows the port to receive tagged and untagged VLAN
tagged	Allows the port to receive only tagged VLAN packets.

Command Default

None

Command Modes

Interface configuration

Examples

This example shows how to configure the **ingress acceptable-frame** command:

```
Device(config)#interface ethernet 1/1
Device(config-if-ethernet-1/1)#ingress acceptable-frame tagged
Config acceptable-frame type successfully!
```

ingress filtering

To enable the forwarding of VLAN packets at the ingress of an interface, use the **igress filtering** command in the Interface configuration mode. To disable ingress filtering use the **no** form of the command.

ingress filtering
no ingress filtering

Syntax Description

ingress filtering	enables ingress filtering of VLAN packets.

Command Default

Ingress filtering is enabled by default

Command Modes

Interface configuration mode

Examples

This example shows how to disable ingress filtering for a port:

```
Device(config)# interface ethernet 1/4
Device(config-if-ethernet-1/4)# no ingress filtering
```

interface ethernet

To enter interface configuration mode for an Ethernet IEEE 802.3 interface, use the interface ethernet command in the global configuration mode.

interface ethernet *port-number*

Syntax Description

port-number	Specifies the port number within a particular slot.

Command Default

None

Command Modes

Global configuration mode

Examples

The following example shows how to enter interface configuration mode.

```
Device(config)# interface ethernet1/4
```

priority

To assign a priority value to a port use the **priority** command in the interface configuration mode. To restore the port priority to the default value use the **no** form of the command.

priority *port-priority*

no priority

Syntax Description

port-priority	Assigns a priority value to the port. The value can range from 0-7.

Command Default

None

Command Modes

Interface configuration mode

Examples

The following example shows how to configure the priority value of a port.

```
Device(config)# interface ethernet1/4
Device(config-if-ethernet-1/4)# priority 2
```

show ingress interface

To display the status of filtering on the ingress port use the **show ingress interface** command in the privileged EXEC mode or global configuration mode.

show ingress interface {**ethernet** *port-number* | **gpon** *port-number*}

Syntax Description

ethernet	Displays information about ethernet port.
gpon	Displays information about gpon port

Command Modes

Privileged EXEC
Global configuration (config)

Examples

The following is sample output for the show ingress interface command.

```
Device(config)#show ingress interface ethernet 1/4
Port     Filtering  Acceptable-frame
e1/4     enable     all
Total entries: 1
```

show interface brief ethernet

To display the configurations of a port in brief use the **show interface brief ethernet** command in the priveleged EXEC mode.

show interface brief ethernet *port-number*

Syntax Description

port-number	Specifies the port for which the configurations will be displayed.

Command Default

None

Command Modes

Priviledged EXEC

Examples

This example shows the sample output for the **show interface brief ethernet** command:

```
Device# show interface brief ethernet 1/4
Port    Desc   Link shutdn Speed         Pri PVID Mode TagVlan    UtVlan
e1/4           down false  auto          2   1    acc             1
Total entries: 1 .
```

show interface ethernet

To display the configurations of a port in detail use the **show interface ethernet** command in the priveleged EXEC mode.

show interface ethernet *port-number*

Syntax Description

port-number	Specifies the port for which the configurations will be displayed.

Command Default

None

Command Modes

Priviledged EXEC

Examples

The following examples displays the output of the **show interface ethernet** command for the port etherent 1 / 4 :

```
Device# show interface ethernet 1/4
Gigabit Ethernet e1/4 current state: enabled, port link is down
 Hardware address is 00:0a:5a:9b:18:15
 SetSpeed is auto, ActualSpeed is unknown, Duplex mode is unknown
 Current port type: 1000BASE-T
 Priority is 2
 Flow control is disabled
 Broadcast storm control target rate is 49984pps
 PVID is 1
 Port mode: access
 Untagged  VLAN ID: 1
 Input  : 0 packets, 0 bytes
          0 broadcasts, 0 multicasts, 0 unicasts
 Output : 0 packets, 0 bytes
          0 broadcasts, 0 multicasts, 0 unicasts
```

switchport default vlan

To configure a VLAN as the default VLAN use the **swithcport default vlan** command in the interface configuration mode. To restore the deafult vlan to port 1 use the **no** form of the command.

switchport default vlan*vlan-id*

no switchport default vlan

Syntax Description

vlan-id	Specifies the VLAN id that will be used as the default VLAN.

Command Default

None

Command Modes

Interface configuration mode

Examples

This example shows how to configure a default vlan:

```
Device(config)# interface ethernet 1/1
Device(config-if-ethernet-1/1)# switchport mode access
Device(config-if-ethernet-1/1)# switchport default vlan 100
```

switchport ethernet

To add an VLAN interface to a designated port or to all ports use the **switchport ethernet** command in the VLAN configuration mode.

switchport {**ethernet** *port-number* | **all**}

Syntax Description

all	Specifies that all the ports will be added to the VLAN interface.
port-number	Specifies the port numbers that will be added to the VLAN interface.

Command Default

None

Command Modes

VLAN configuration

Examples

This example shows how to add a VLAN to an ethernet port:

```
Device(config-if-vlan)# switchport ethernet 1/4
```

switchport hybrid

To allow the packets from specified VLANs to pass through the hybrid port, use the **switchport hybrid** command in the interface configuration mode. To prevent the packets from specified VLANs passing through the hybrid port use the **no** form of the command.

switchport hybrid { **tagged** | **untagged** } **vlan** { *vlan-list* | **all** }

no switchport hybrid { **tagged** | **untagged** } **vlan** { *vlan-list* | **all** }

Syntax Description

tagged	Specifies the VLAN packets as tagged.
untagged	Specifies the VLAN packets as untagged.
vlan	Specifies the VLANs whose packets will be allowed to pass through the hybrid port.
vlan-list	Specifies a list of VLANs whose packets will be allowed to pass through the hybrid port.
all	Specifies that packets from all VLANs will be allowed to pass through the hybrid port.

Command Default

None

Command Modes

Interface configuration mode

Examples

This example shows how to allow the packets from the specified VLANs to pass through the hybrid port:

```
Device(config-if-ethernet-1/4)# switchport mode hybrid
Device(config-if-ethernet-1/4)# switchport hybrid tagged 2-4
```

switchport mode

To configure the VLAN mode for the interface use the **switchport mode** command in the interface configuration mode. You can set the VLAN mode to access, hybrid or trunk. The mode is set to hybrid by default.

switchport mode { **access** | **hybrid** | **trunk** }

Syntax Description

access	Specifies that the interface is in access mode.
hybrid	Specifies that the interface is in hybrid mode.
trunk	Specifies that the interface is in trunk mode.

Command Default

None

Command Modes

Interface configuration

Examples

This example shows how to configure the VLAN mode to trunk on an interface:

```
Device(config)# interface ethernet1/4
Device(config-if-ethernet-1/4)# switchport mode trunk
```

switchport trunk

To allow the packets from specified VLANs to pass through the trunk port, use the **switchport trunk** command in the interface configuration mode. To prevent the packets from specified VLANs passing through the hybrid port use the **no** form of the command.

switchport trunk allowed vlan { *vlan-list* | **all** }

no switchport trunk allowed vlan { *vlan-list* | **all** }

Syntax Description

allowed	Configures the VLANs whose packets will be allowed to pass through the trunk port.
vlan	Specifies the VLANs whose packets will be allowed to pass through the trunk port.
vlan-list	Specifies VLAN IDs of the allowed VLANs when the interface is in trunking mode.
all	Specifies all VLANs to be added to the current list.

Command Default

None

Command Modes

Interface configuration

Examples

This example shows how to allow the packets from the specified VLANs to pass through a trunk port:

```
Device(config-if-ethernet-1/4)# switchport mode trunk
Device(config-if-ethernet-1/4)# switchport trunk allowed vlan 2-4
```

vlan

To add a VLAN and to enter the VLAN configuration mode, use the **vlan** command in global configuration mode. To delete the VLAN, use the **no** form of this command.

vlan *vlan list*

no vlan *vlan list*

Syntax Description

vlan list	List of VLAN to be added and configured.The range is 1 to 4094.You can enter a single VLAN ID, a series of VLAN IDs separated by commas, or a range of VLAN IDs separated by hyphens.

Command Default

None

Command Modes

Global Configuration

Examples

This example shows how to create a VLAN and enter the VLAN configuration mode:

```
Device(config)# vlan 1
```

PART V

OLT Network Configuration

OLT Network Configuration

arp

To add a static entry in the Address Resolution Protocol (ARP) table, use the **arp** command in the global configuration mode. To remove an entry from the ARP table, use the **no** form of the command.

[**no**] **arp***ip-address* **mac***mac-address* [**vid** *vlan-id* | **port** *port-id*]

Syntax Description

ip-address	IPv4 address for which a permanent entry is added to the ARP table. Enter the IPv4 address in a four-part dotted-decimal format that corresponds to the local data-link address (a 32-bit address)
mac *mac-address*	Hardware MAC address that the IPv4 address is linked to. Enter the MAC address in dotted-hexadecimal notation.
vid *vlan-id*	(Optional) Specifies the configured VLAN.
port *port-id*	(Optional) Specifies the configured port

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

You can manually configure and maintain a static ARP entry. It cannot be aged or overwritten by dynamic ARP entry. A static ARP entry can be a long or a short entry. A static ARP entry comprises IP address and the corresponding MAC address. A long static ARP entry comprises the VLAN and egress interface details along with the IP address and MAC address. Long Static ARP entries can be directly used for packet forwarding.

When you manually configure a Long Static ARP entry, the IP address in the entry must be in the same network segment as the IP address of the VLAN interface on which the egress interface resides.

A short static ARP entry comprises the IP Address and the MAC Address. A short static ARP entry cannot be directly used for packet forwarding. A shorts static ARP request packet is sent by the host. If the source IP address and the source MAC address in the received response packet are the same as the configured IP address and MAC address, the ARP entry will be completed. Then it can be used for packet forwarding.

Example

This example shows how to configure a short static ARP entry:

```
Device> enable
Device# configure terminal
Device(config)# arp 192.168.1.19 mac 00:02:9a:3b:94:d9
```

arp aging-time

To specify how long an entry can exist in an ARP table, use the **arp aging-time** command in the global configuration mode.

arp aging-time *aging-time*

Syntax Description

aging-time	Specify the timeout period in seconds.

Command Default

The default timeout of an ARP table entry is 20 minutes.

Command Modes

Global configuration (config)

Example

This example shows how to configure the aging time for ARP table entries:

```
Device> enable
Device# configure terminal
Device(config)# arp aging-time 300
```

description *interface-name*

To configure the interface description, use the **description** *interface name* in the VLAN configuration mode. You can delete the interface description by using the**no** form of the command.

description *interface-name*

no description *interface-name*

Syntax Description

interface-name	Adds a description for the interface.

Command Default

None

Command Modes

VLAN configuration

Examples

The following example shows how to configure the IP interface description

```
Device(config-if-vlanif)# description interface1
```

dhcp-snooping

To enable Dynamic Host Control Protocol (DHCP) snooping feature on a device, use the **dhcp-snooping** command in the global configuration mode.

dhcp-snooping [**port-down-action fast-remove**]

Syntax Description

port-down-action fast-remove	Configures the link down operation on the port.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

When DHCP Snooping is enabled on your device, it monitors and validates the DHCP packets that it receives. Untrusted ports drop the DHCP-ACK and DHCP-OFFER packets that are received from DHCP servers. Trusted ports forward the received DHCP packets to DHCP clients.

To configure DHCP Snooping feature, use the **dhcp-snooping** command.

When a link in the network goes down, use the **dhcp-snooping port-down-action fast remove** command to remove the corresponding entry from the DHCP binding database.

Example

This example shows how to configure DHCP Snooping on a device:

```
Device> enable
Device# configure terminal
Device(config)# dhcp-snooping
```

dhcp-snooping trust

To configure an interface as trusted for Dynamic Host Control Protocol (DHCP) snooping operations, use the **dhcp-snooping trust** command in the interface configuration mode.

dhcp-snooping trust

Command Default None

Command Modes Global configuration (config)

Example

This example shows how to configure a trusted interface for DHCP Snooping:

```
Device> enable
Device# configure terminal
Device(config)# interface g0/1
Device(config-if)# dhcp-snooping trust
```

dhcpv6-snooping

To enable Dynamic Host Control Protocol version 6 (DHCPv6) snooping feature on a device, use the **dhcpv6-snooping** command in the global configuration mode.

dhcpv6-snooping [**port-down-action fast-remove**]

Syntax Description

port-down-action fast-remove	Configures the link down operation on the port.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

When DHCPv6 Snooping is enabled on your device, it monitors and validates the DHCP packets that it receives. Untrusted ports drop the DHCP-ACK and DHCP-OFFER packets that are received from DHCP servers. Trusted ports forward the received DHCP packets to DHCP clients.

To configure DHCPv6 Snooping feature, use the **dhcpv6-snooping** command.

When a link in the network goes down, use the **dhcpv6-snooping port-down-action fast remove** command to remove the corresponding entry from the DHCP binding database.

Example

This example shows how to configure DHCPv6 Snooping on a device:

```
Device> enable
Device# configure terminal
Device(config)# dhcpv6-snooping
```

dhcpv6 snooping port-down-action fast-remove

To configure the link-down operation on the port, use the **dhcp-snooping port-down-action fast-remove** command in the interface configuration mode.

dhcp-snooping port-down-action fast remove

Command Default None

Command Modes Global configuration (config)

Example

This example shows how to configure the link-down operation on the port:

```
Device> enable
Device# configure terminal
Device(config)# dhcp-snooping port-down-action fast-remove
```

dhcpv6-snooping trust

To configure an interface as trusted for DHCPv6 snooping operations, use the **dhcpv6-snooping trust** command in the interface configuration mode.

dhcpv6-snooping trust

Command Default None

Command Modes Global configuration (config)

Example

This example shows how to configure a trusted interface for DHCPv6 Snooping:

```
Device> enable
Device# configure terminal
Device(config)# interface g0/1
Device(config-if)# dhcpv6-snooping trust
```

dlf forward

To enable the forwarding of Destination Lookup Failure (DLF) unicast or multicast packets, use the **dlf forward** command. To enable DLF forwarding on egress packets of all ports, use the command in the global configuration mode. To enable DLF forwarding on the egress packets of a specific port, use the command in the interface configuration mode. DLF Forwarding is disabled by default. To disable it use the **no** form of the command.

dlf-forward { **unicast** | **multicast** }

no dlf-forward { **unicast** | **multicast** }

Syntax Description

unicast	Enables the forwarding function of DLF unicast packets
multicast	Enables the forwarding function of DLF multicast packets

Command Default

DLF forwarding is disabled by default.

Command Modes

Global configuration mode.
Interface configuration mode.

Examples

The following example shows how to configure DLF forwarding for unicast packets for all egress ports:

```
Device(config)# dlf-forward unicast
```

The following example shows how to configure DLF forwarding for unicast packets on a specific port:

```
Device(config)# interface ethernet 1/4
       Device(config-if)# dlf-forward unicast
```

The following example shows how to configure DLF forwarding for multicast packets for all egress ports:

```
Device(config)# dlf-forward multicast
```

The following example shows how to configure DLF forwarding for multicast packets on a specific port:

```
Device(config)# interface ethernet 1/4
       Device(config-if)# dlf-forward multicast
```

clear dhcpv6-snooping

To delete the dynamic entries that is recorded by DHCPv6 Snooping, use the **clear dhcpv6-snooping** command in global configuration mode.

clear dhcpv6-snooping { **ip** *address* | **mac** *mac_address* | **vlan** *vlan_id* | **interface ethernet** *slot-num/pon-num/ont-num* }

Syntax Description

address	Specifies the IPv6 address entry
mac_address	Specified the MAC address entry
vlan_id	Specifies the VLAN ID entry
slot-num/pon-num/ont-num	Specifies the ethernet port entry

Command Default

None

Command Modes

Global Configuration (config)

Example

The following example shows a sample format of the output of this command:

```
Device(config)# clear dhcpv6-snooping
```

interface

To configure an interface and enter into Interface configuration mode, use the **interface** command in the global configuration mode.

interface {*port-id* | **ethernet** *slot-num/port-num* | **gpon** *slot-num/port-num* | **loopback-interface** *loopback-int-number* | **meth-interface** *meth-int-number* | **range** {**ethernet** *port-num/slot-num* | **gpon** *port-num/slot-num* } | **vlan-interface** *vlan-id* }

Syntax Description

port-id	Specifies the port to be configured. It is a string consisting of 4 to 14 characters.
ethernet *slot-num/port-num*	Enables you to configure Ethernet ports. For a Gigabit Ethernet port, *slot-num* is 1 and *port-num* ranges from 1 through 4. For a Ten Gigabit Ethernet port, *slot-num* is 2 and *port-num* ranges from 1 through 2.
gpon *slot-num/port-num*	Enables you to configure GPON ports. *slot-num* is 0 and *port-num* ranges from 1 through 8.
loopback-interface *loopback-int-number*	Enables you to configure a loopback interface. *loopback-int-number* number can be 0 or 1.
meth-interface *meth-int-number*	Enables you to configure the Management Interface, MEth, that allows you to log in and perform configurations.
range {**ethernet** *port-num/slot-num* | **gpon** *port-num/slot-num* }	Enables you to configure a range of ethernet interfaces or a range of GPON interfaces.
vlan-interface *vlan-id*	Enables you to configure a VLAN interface. *vlan-id* specifies the VLAN id. Values range from 1 through 4094.

Command Modes

Global Configuration (config)

Command Default

None

Usage Guidelines

Use the **interface** command to enter the Interface Configuration mode and configure the interface.

To configure a range of interfaces at once, use the **interface range** command. In the interface range configuration mode, all entered commands are applicable to all interfaces within that range.

Example

The following example configures an Ethernet interface:

```
Device#configure terminal
Device(config)#interface ethernet 1/1
Device(config-if-ethernet-1/1)#
```

The following example configures a range of GPON interfaces:

```
Device#configure terminal
Device(config)#interface range gpon 0/1 to gpon 0/3
```

interface loopback-interface

To create a loopback interface and to enter the loopback interface configuration mode, use the **interface loopback-interface** command in the Global configuration mode.

To disable a loopback interface use the **no** form of the command.

interface loopback-interface *interface-number*

no interface loopback-interface

Syntax Description

loopback-interface	Configures a loopback interface.
interface-number	Configures the loopback interface number.

Command Default

None

Command Modes

Global configuration mode

Examples

The following example shows how to configure a loopback interface:

```
Device(config)# interface loopback-interface 1
```

interface vlan-interface

To create a VLAN interface and enter interface configuration mode, use the **interface vlan-interface** command in the global configuration mode. To remove a VLAN interface, use the **no** form of the command.

interfacevlan-interface *vlan-id*

no interfacevlan-interface

Syntax Description

vlan-id	Sets the VLAN for the interface. The range is from 1-4094.

Command Default

None

Command Modes

Global configuration

Examples

The following example shows how to configure an interface VLAN:

```
Device(config)# interface vlan-interface 1
```

ip-source-guard

To enable IP Source Guard feature on a device, use the **ip-source-guard** command in the global configuration mode.

ip-source-guard { **vlan** *vlan-list* | **permit igmp** | **bind ip** *ip-address* [**mac** *mac-address* **interface** { **ethernet** | **gpon** } *interface-id* **vlan** *vlan-id*] }

Syntax Description

vlan *vlan-list*	Configures IP Source Guard on the VLANs listed by *vlan-list*.
permit igmp	Configures IP Source Guard to allow Internet Group Management Protocol (IGMP) packets to pass through.
bind ip *ip-address*	Configures an entry in the static IP source binding table.
mac *mac-address*	The MAC address that is bound to the IP address.
interface	Specifies the interface to be configured.
ethernet	Specifies the Ethernet interface
gpon	Specifies the GPON interface
vlan *vlan-id*	Specifies the VLAN to which the interface belongs.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

IP Source Guard feature filters the source IP address on a Layer 2 port to prevent a malicious host from impersonating a legitimate host.

You can enable the IP Source Guard feature only on untrusted ports. For IP Source Guard to function, enable DHCP Snooping.

Use the **ip-source-guard bind** command to configure an IP source binding.

Use the **ip-source-guard vlan** *vlan-list* command to configure IP Source Guard on the listed VLANs.

Use the **ip-source-guard permit igmp** command to allow IGMP packets to pass through.

Example

The following example shows how to configure an entry in the IP source binding table:

```
Device> enable
Device# configure terminal
Device(config)# ip-source-guard bind ip 192.168.11.2
```

The following example shows how to configure ip source guard on three VLANs:

```
Device(config)# ip-source-guard vlan 7,8,10
```

ip-source-guard filter

To configure the port filtering mode for an interface, use the **ip-source-guard** command in the interface configuration mode.

```
ip-source-guard [ip |ip-mac | ip-mac-vlan]
```

Syntax Description

ip	Specifies that the port filter packets are based on source IP, regardless of the MAC address and the VLAN ID.
ip-mac	Specifies that the port filters packets based on the source IP address and the MAC address of the packet.
ip-mac-vlan	Specifies that the port filters packets based on source IP address, MAC address, and VLAN ID.

Command Default

None

Command Modes

Interface Configuration (config-if)

Usage Guidelines

IP Source Guard feature filters the source IP address on a Layer 2 port to prevent a malicious host from impersonating a legitimate host.

You can enable the IP Source Guard feature only on untrusted ports. For IP Source Guard to function, enable DHCP Snooping.

Use the **ip-source-guard ip** command on the interface to filter packets are based on source IP, regardless of the MAC address and the VLAN ID.

Use the **ip-source-guard ip-mac** *vlan-list* command on the interface to filter packets are based on source IP and MAC address, regardless of the VLAN ID.

Use the **ip-source-guard ip-mac-vlan** command on the interface to filter packets are based on source IP, MAC address,and VLAN ID.

If you don't specify the port filtering mode, the port filters packets based on the source IP address, MAC address, and VLAN ID.

Example

The following example shows how to configure the port to filter packets based on the source IP address and MAC address:

```
Device> enable
Device# configure terminal
Device(config)# interface etherent 1/1

Device(config-if-ethernet-1/1)# ip-source-guard ip-mac
Config IP source guard mode of port successfully.
```

ip address

To configure the primary IP address for the VLAN interface, use the **ip address** command in the VLAN configuration mode.

ip address { *ip-addressmask-ip-address***override** | **primary** *ip-address* }

Syntax Description

Override	Overrides the IP address of the VLAN interface.
primary	Configures the primary IP address for the VLAN interface.

Command Default

None

Command Modes

VLAN configuration

Examples

The following example shows how to configure the pimary IP address for an interface:

```
Device(config-if-vlan)# ip address primary 192.0.2.1
```

ip address *mask-ip-address*

To configure a loopback interface for the IP address, use the **ip address** *mask-ip-address* command in the loopback interface configuration mode.

To disable the loopback loopback interface for the IP address, use the **no** form of the command.

ip address*ip-address mask-ip-address*

no ip address*ip-address mask-ip-address*

Syntax Description

ip-address	It is the IP address of the interface
mask-ip-address	Configures the loopback IP address for the interface.

Command Default

None

Command Modes

Loopback interface configuration mode

Examples

The following example shows how to configure a loopback interface for the IP address

```
Device(config-if-loopbackinterface)# ip address 192.0.2.1 255.255.255.0
```

ip address range

To configure the range of IP addresses for the VLAN interface, use the **ip address range** command in the the VLAN configuration mode. You can delete the range of IP addresses for the VLAN interface using the **no** form of the command.

ip address range { *start-ip-address end-ip-address* }

no ip address range { *start-ip-address end-ip-address* }

Syntax Description

range	Configures the range of IP addresses for the VLAN interface
start-ip-address	Configures the starting IP address of the range.
end-ip-address	Configures the ending IP address of the range.

Command Default

None

Command Modes

VLAN configuration mode

Examples

The following example shows how to configure a range of IP addresses for the interface:

```
Device(config-if-vlan)# ip address range 192.0.2.254 192.0.2.255
```

ip icmp mask-reply

To enable the ICMP address mask reply packet, use the **ip icmp mask-reply** command in the global configuration mode. To disable the ICMP address mask reply packet, use the **no** form of the command.

ip icmp mask-reply

no ip icmp mask-reply

Syntax Description

mask-reply	Enables the ICMP address mask reply packet.

Command Default

None

Command Modes

Global configuration mode

Examples

The following example shows how to enable ICMP address mask reply packet:

```
Device(config)# ip icmp mask-reply
```

ip icmp unreachable

To enable the sending of ICMP destination unreachable packets, use the **ip icmp unreachable** command in the VLAN configuration mode. To disable the sending of ICMP destination unreachable packets, use the **no** form of the command.

ip icmp unreachable

no ip icmp unreachable

Syntax Description

unreachable	Enables the sending of ICMP destination unreachable packets.

Command Default

None

Command Modes

VLAN configuration mode

Examples

The following example shows how to enable the sending of ICMP destination unreachable packets.

```
Device(conifg-if-vlanif)# ip icmp unreacheable
```

ipv6 address

To configure the IPv6 address for the VLAN interface, use the **ipv6 address** command in the VLAN configuration mode. To delete the IPv6 address use the **no** form of the command.

ipv6 address { *ipv6-address-mask ipv6-address/prefixlength* | **autoconfig** }

no ipv6 address { *ipv6-address-mask ipv6-address/prefixlength* | **autoconfig** }

Syntax Description

ipv6-address/prefixlength	Specifies the IPv6 prefix for the VLAN interface.
ipv6-address-mask	Specifies the IPv6 destination address for the VLAN interface.
autoconfig	Enables stateless autoconfiguration.

Command Default

None.

Command Modes

VLAN configuration

Examples

The following example shows how to configure the IPv6 address for an interface:

```
Device> enable
Device# configure terminal
Device(config)# inteface vlan-interface 100
Device(config-if-vlan)# ipv6 address 2001::100/64
```

ipv6 address link-local

To specify the link local address manually on a VLAN interface, use the **ipv6 address link-local** command in the VLAN configuration mode. The link-local is automatically formed by default.

ipv6 address *ipv6-address* **link-local**

Syntax Description

ipv6-address	Specifies the IPv6 prefix for the VLAN interface.
link-local	Configures a link-local IPv6 address.

Command Default

The link-local is automatically formed by default.

Command Modes

VLAN configuration

The following example shows how to configure a link-local IPv6 address on a VLAN interface using the **ipv6 address link-local** command.

```
Device> enable
Device#configure terminal
Device(config)# ipv6 enable
Device(config)# interface vlan-interface 1
Device(config-vlan-if)# ipv6 address FE80:1::100 link-local
```

ipv6 enable

To enable IPv6 forwarding, use the **ipv6 enable** command in global configuration mode. To disable IPv6 forwarding, use the **ipv6 disable** command in global configuration mode.

ipv6 { **enable** | **disable** }

Syntax Description

enable	Enables IPv6 forwarding.
disable	Disables IPv6 forwarding.

Command Modes

Global configuration (config)

The following example shows how to enable IPv6 forwarding using the **ipv6 enable** command:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 enable
```

ipv6 icmpv6 multicast-echo-reply

To enable an echo-reply for an echo request, use the **ipv6 icmpv6 multicast-echo-reply** command in global configuration mode. You can use the **no ipv6 icmpv6 multicast-echo-reply** command to disable reply for multicast packets.

ipv6 icmpv6 multicast-echo-reply enable

no ipv6 icmpv6 multicast-echo-reply

Syntax Description

enable	Enables echo reply for multicast packets

Command Default

None.

Command Modes

Global configuration mode (config)

The following example shows how to enable echo reply for multicast packets by using the **ipv6 icmpv6 multicast-echo-reply enable** command in global configuration mode.

```
Device> enable
Device# configure terminal
Device(config)# ipv6 icmpv6 multicast-echo-reply enable
```

ipv6 nd dad attempts

To configure the number of times Neighbor Solicitation (NS) messages will be sent for duplicate address detection, use the **ipv6 nd dad attempts** command in global configuration mode. You can use the **no ipv6 nd dad attempts** command to configure the number of NS messages sent to the value of 0.

ipv6 nd dad attempts *value*

no ipv6 nd dad attempts

Syntax Description

value	Configures the number of times NS messages are sent for duplicate address detection. The value ranges from 0 to 20. the default value for the number of NS messages sent is 1. When value is 0, it implies duplicate address detection is disabled

Command Default

None.

Command Modes

Global configuration mode (config)

The following example shows how to configure the number of NS messages sent for duplicate address detection to 10, using the **ipv6 nd dad attempts** command in global configuration mode.

```
Device> enable
Device# configure terminal
Device(config)# ipv6 nd dad attempts 10
```

ipv6 nd ns retrans-time

To set the time interval for retransmitting the Neighbor Solicitation (NS) message, use the **ipv6 nd ns retrans-time** command in global configuration mode. You can use the **no ipv6 nd ns retrans-time** command to disable the retransmission timer.

ipv6 nd ns retrans-time *value*

no ipv6 nd ns retrans-time

Syntax Description

value	Sets the time interval for retransmitting the NS message. The value ranges from 1 to 3600 seconds. The default value for retransmitting the NS message is 1 second.

Command Default

None.

Command Modes

Global configuration mode (config)

The following example shows how to set the time interval for retransmitting the NS messgae to 60 seconds using the **ipv6 nd ns retrans-time** command in global configuration mode.

```
Device> enable
Device# configure terminal
Device(config)# ipv6 nd ns retrans-time 60
```

ipv6 nd reachable-time

To configure the time for which a neighbor is considered to be in a reachable state, use the **ipv6 nd reachable-time** command in the global configuration mode. You can use the **no ipv6 nd reachable-time** command to reset the reachable time to its default value of 30 seconds.

ipv6 nd reachable-time *value*

no ipv6 nd reachable-time

Syntax Description

value	Configures the time for which a neighbor is considered to be in a reachable state. The value ranges from 1-3600 seconds. The default value is 30 seconds.

Command Default

The default value of the reachable time is 30 seconds.

Command Modes

Global configuration mode (config)

The following example shows how to configure the reachable-time to 60 seconds, using the **ipv6 nd reachable-time** command in global configuration mode.

```
Device> enable
Device# configure terminal
Device(config)# ipv6 nd reachable-time 60
```

ipv6 neighbors max-learning-num

To configure the maximum number of neighbors that can access an IPv6 address, use the **ipv6 neighbors max-learning-num** command in the global configuration mode. The maximum neighbor number includes both static and dynamic neighbors. You can use the **no ipv6 neighbors max-learning-num** command to reset the maximum number of neighbors to the default value of 64.

ipv6 neighbors max-learning-num *number*

no ipv6 neighbors max-learning-num

Syntax Description

number	Configures the maximum number of neighbors for an IPv6 address. The range for the number is 1 to 2560. The default maximum number of neighbors is 64.

Command Default

The default maximum number of neighbors is 64.

Command Modes

Global configuration mode (config)

The following example shows how to configure the maximum neighbor number to 1000 using the **ipv6 neighbors max-learning num** command in global configuration mode.

```
Device> enable
Device# configure terminal
Device(config)# ipv6 neighbors max-learning-num 1000
```

ipv6 path

To configure the Maximun Transimssion Unit (MTU) value for an IPv6 interface, use the **ipv6 path** command in the VLAN interface configuration mode. You can use the **no ipv6 path** command to reset the MTU value to its default value of 1500.

ipv6 path *mtu-value*

no ipv6 path *mtu-value*

Syntax Description

mtu-value	Configures the MTU for the IPv6 interface. The MTU value ranges from 1280-1500. The default MTU value is 1500.

Command Default

The default MTU value is 1500 .

Command Modes

VLAN configuration

The following example shows how to set the MTU value to 2000 for an IPv6 interface, using the **ipv6 path** command in VLAN configuration mode.

```
Device> enable
Device# configure terminal
Device(config)# inteface vlan-interface 100
Device(config-vlan_if)# ipv6 path 2000
```

ipv6 route

To configure a static route with the IPv6 address, use the **ipv6 route** command in global configuration mode. To disable static route, use the **no** form of the command.

ipv6 route { *ipv6-address/prefixlength ipv6-address/prefixlength* } *next-hop-address*

no ipv6 route { *ipv6-address/prefixlength ipv6-address/prefixlength* } *next-hop-address*

Syntax Description

ipv6-address/prefixlength	Specifies the IPv6 prefix.
ipv6-address/prefixlength	Specifies the IPv6 destination address.
next-hop-address	Specifies the IPv6 next hop address.

Command Default

None.

Command Modes

Global configuration (config)

Examples

The following example shows how to configure a static route using the **ipv6 route** command:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 route 2001:DB8:1::0/64 2001:DB8:0:ABCD::1
```

no ipv6 neighbor

To delete neigbors from the ipv6 neighbors list, use the **no ipv6 neighbor** command in global configuration mode.

no ipv6 neighbor { **dynamic** | **static** | **all** }

Syntax Description

dynamic	Deletes the dynamic neighbors from the IPv6 neighbor list.
static	Deletes the static neighbors from the IPv6 neighbor list.
all	Deletes all the neighbors from the IPv6 neighbor list.

Command Default

None.

Command Modes

Global configuration (config)

The following example shows how to all the dynamic neighbors from the IPv6 neigbor list by using the **no ipv6 neighbor** command in the global configuration mode.

```
Device> enable
Device#configure terminal
Device(config)# no ipv6 neighbor dynamic
```

mac-address-table

To add a MAC address manually to the MAC address table, use the **mac-address-table** command in the global configuration mode. To remove a MAC address from the table, use the **no** form of the command.

mac-address-table {**static** | **permanent** | **dynamic**} *mac-address* **interface ethernet***interface-number* **vlan** *vlan-id*

no mac-address-table {**static** | **permanent** | **dynamic**} *mac-address* **interface ethernet***interface-number* **vlan** *vlan-id*

Syntax Description

static	Adds a static MAC address to the MAC address table.
permanent	Adds a MAC address permanently to the MAC address table.
dynamic	Adds a dynamic MAC address to the MAC address table.

Command Default

None

Command Modes

Global configuration

Examples

The following examples shows how to add a static MAC address to a MAC address table:

```
Device(config)# mac-address-table static 00:50:3e:8d:64:00 interface ethernet
 1/4 vlan 3
```

mac-address-table learning

To disable dynamic MAC address learning, use the **no mac-address-table learning** command. To disable MAC address learning on all ports use the command in the global configuration mode. To disable MAC address learning on specific ports use the command in the interface configuration mode. MAC address learning is enabled by default.

mac-address-table learning

no mac-address-table learning

Syntax Description

learning	Enables or disables MAC address learning.

Command Default

MAC address learning is enabled by default.

Command Modes

Global configration
Interface configuration

Examples

The folowing example shows how to disable MAC address learning on an ethernet port:

```
Device(config)# interface ethernet 1/4
Device(config-if-ethernet-1/4)# no mac-address-table learning
```

mac-address-table age-time

To configure the aging time for entries in the MAC address table, use the **mac-address-table age-time** command in the global configuration mode. To disable the aging process use the **disable** keyword.

mac-address-table age-time {*seconds* | **disable**}

Syntax Description

disable	Disables the ageing process for the MAC address table.
seconds	Configures the ageing time for the MAC address table in seconds.

Command Default

None

Command Modes

Global configuration

Examples

The following example shows how to configure ageing time for a MAC address table:

```
Device(config)# mac-address-table age-time 120
```

mac-address-table blackhole

To add the MAC address of an untrusted user as a Blackhole MAC address, use the **mac-address-table blackhole** command in the global configuration mode. To remove a MAC addeess as a Blackhole MAC address use the **no** form of the command.

mac-address-tableblackhole *mac-address* **vlan** *vlan-id*

no mac-address-tableblackhole *mac-address* **vlan** *vlan-id*

Syntax Description

blackhole	Adds a MAC address as a Blackhole MAC address.

Command Default

None

Command Modes

Global configuration

Examples

The following example shows how to add a MAC address as a Blackhole MAC address:

```
Device(config)# mac-address-table blackhole 00:05:00:05:00:05 vlan 1
```

mac-address-table max-mac-count

To configure the maximum number of MAC addresses that will be learnt by the MAC Address Table on a port, use the **mac-address-table max-mac-count** command in the interface configuration mode. To keep the number of MAC addresses learnt as unlimited use the **no** form of the command. By default, the number of MAC addresses that are dynamically learnt by the MAC Address Table are unlimited.

mac-address-table max-mac-count *integer*

no mac-address-table max-mac-count *integer*

Syntax Description

max-mac-count *integer*	Enables a limit on the number of dynamically learnt MAC addresses added to the table

Command Default

The number of learnt MAC addresses are unlimited by default

Command Modes

Interface configuration

Examples

The following example shows how to enable a maximum learnt MAC address count on a port:

```
Device(config)# interface ethernet 1/4
Device(config-if-ethernet-1/4)# mac-address-table max-mac-count 500
```

mirror destination-interface

To configure a port as destination port for mirroring, use the mirror destination-interface command in the global configuration mode. To remove the mirroring configuration, use the **no** form of the command.

[**no**] **mirror destination-interface** {**ethernet** *slot/port* | **gpon** *slot/port*}

Syntax Description

ethernet *slot/port*	Specifies the ethernet interface that can be configured as the destination for port mirroring
gpon *slot/port*	Specifies the GPON interface as the destination for port mirroring.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

Use this command to configure the destination port that receives the mirrored packets.

Port mirroring duplicates the data packets on the monitored (source) port and sends the packets to a destination port for monitoring or analysis. You can mirror inbound packets or outbound packets or both types of packets on the source port.

A port configured as a destination port cannot be used as a normal port.

For a switch, you can configure only one port as destination port.

Example

The following example sets the ethernet port 2/1 as the destination for mirroring.

```
Device#configure terminal
Device(config)#mirror source-interface ethernet 1/1 both

Device(config)#mirror destination-interface ethernet 2/1
```

mirror source-interface

To configure a port to act as a source port for mirroring, use the **mirror source-interface** command in the global configuration mode. To remove the mirroring configuration, use the **no** form of the command.

[**no**] **mirror source-interface** {**ethernet** *slot/port* | **cpu** | **gpon** *slot/port* } {**ingress** | **egress** | **both**}

Syntax Description

ethernet *slot/port*	Specifies the ethernet interface that can be configured as the source for port mirroring
cpu	Specifies the CPU as the source for port mirroring
gpon *slot/port*	Specifies the GPON interface as the source for port mirroring.
ingress	Specifies that the packets at the ingress of the specified port, which are inbound, are mirrored.
egress	Specifies that packets at the egress of the specified port, which are outbound, are mirrored.
both	Specifies that the packets at both the ingress and egress interfaces are mirrored.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

Use this command to configure the source port for mirroring the packets at the port. You can mirror inbound packets or outbound packets or both types of packets.

Port mirroring duplicates the data packets on the monitored (source) port and sends the packets to a destination port for monitoring or analysis.

You can configure multiple ports as source port for mirroring.

Example

The following example sets the ethernet port 1/1 as the source for mirroring the packets.

```
Device#configure terminal
Device(config)#mirror source-interface ethernet 1/1 both
```

show arp

To display the Address Resolution Protocol (ARP) table entries, use the **show arp** command in privileged or global configuration mode.

show arp {**dynamic** | **static** | **all** }

Syntax Description

dynamic	Displays all the dynamic ARP table entries
static	Displays all the static ARP table entries
all	Displays all the entries from the ARP table

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Usage Guidelines

The **show arp dynamic** command displays all mappings and information about each entry in the ARP table, including the aging time, VLAN instance, and port.

Example

```
Device#show arp dynamic
Informations of ARP
d - days, h - hours, m - minutes, s - seconds
IpAddress       Mac_Address        Vlan  Port     VPTag Type     ExpireTime   Status
10.75.171.1     00:23:5d:fd:94:00  100   e1/3     0     dynamic  18m34s       valid
10.75.171.71    00:50:56:92:1d:fb  100   e1/3     0     dynamic  10m51s       valid
10.75.171.79    00:0c:29:80:8b:59  100   e1/3     0     dynamic  17m43s       valid
10.75.171.91    00:0c:29:71:b1:4f  100   e1/3     0     dynamic  10m59s       valid
10.75.171.138   00:0c:29:f9:35:c3  100   e1/3     0     dynamic  11m07s       valid

Total entries:5
```

Table 5: Description of the show arp dynamic Command Output

IPAddress	Specifies the IP address of the ARP table entry
MAC_Address	Specifies the MAC address associated with the IP address
Vlan	Specifies the VLAN to which this interface belongs
Port	Specifies the port that has learnt the ARP entry
VPTag	Specifies the virtual port for GPON routing
Type	Specifies whether it is a dynamic or a static entry
Expire Time	Displays the time remaining before the ARP entry expires
Status	Specifies whether the entry is valid or not.

show dhcp-snooping clients

To display binding between the IP address and the MAC address that is recorded by DHCP Snooping, use the **show dhcp-snooping clients** command in privileged or global configuration mode.

show dhcp-snooping clients

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Example

The following example shows a sample format of the output of this command:

```
Device#show dhcp-snooping clients
DHCP client information:
d - days, h - hours, m - minutes, s - seconds
IPAddress        mac               vlan  port     LeaseTime      ExceedTime

Total entries: 0. Printed entries: 0.
```

Related Commands

Command	Description
dhcp-snooping	Enables DHCP Snooping on the device.

show dhcp-snooping interface

To display the details of DHCP Snooping on an interface, use the **show dhcp-snooping interface** command in privileged or global configuration mode.

show dhcp-snooping interace [**ethernet** | **gpon**] [*interface-id*]

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Usage Guidelines

This command displays the DHCP Snooping enabled state, information on the trusted port, the number of DHCP clients allowed on the physical port, and the number of currently connected DHCP clients.

Example

```
Device#show dhcp-snooping interface
Config information of DHCP Snooping:
DHCP Snooping status:Enable
DHCP Snooping port-down-action fast-remove:Enable
Port information:
Port          mode      maxclients    clients(ack)  clients(unack)
g0/1          untrust   2048          0             0
g0/2          untrust   2048          0             0
g0/3          untrust   2048          0             0
g0/4          untrust   2048          0             0
g0/5          untrust   2048          0             0
g0/6          untrust   2048          0             0
g0/7          untrust   2048          0             0
g0/8          untrust   2048          0             0
e1/1          untrust   2048          0             0
e1/2          untrust   2048          0             0
e1/3          untrust   2048          0             0
e1/4          untrust   2048          0             0
e2/1          untrust   2048          0             0
e2/2          untrust   2048          0             0


Device#show dhcp-snooping interface gpon 0/1

Config information of DHCP Snooping:
DHCP Snooping status:Enable
DHCP Snooping port-down-action fast-remove:Enable
Port information:
Port          mode      maxclients    clients(ack)  clients(unack)
g0/1          untrust   2048          0             0


Device#show dhcp-snooping interface ethernet 1/1

Config information of DHCP Snooping:
DHCP Snooping status:Enable
DHCP Snooping port-down-action fast-remove:Enable
Port information:
Port          mode      maxclients    clients(ack)  clients(unack)
```

```
e1/1            untrust    2048           0              0
```

show dhcpv6-snooping clients

To display binding between the IP address and the MAC address that is recorded by DHCPv6 Snooping, use the **show dhcpv6-snooping clients** command in privileged or global configuration mode.

show dhcpv6-snooping clients

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Example

The following example shows a sample format of the output of this command:

```
Device#show dhcpv6-snooping clients
DHCPv6 client information:
d - days, h - hours, m - minutes, s - seconds
IPAddress        mac               vlan  port     LeaseTime      ExceedTime

Total entries: 0. Printed entries: 0.
```

Related Commands

Command	Description
dhcpv6-snooping	Enables DHCPv6 Snooping on the device.

show dhcpv6-snooping interface

To display the details of DHCPv6 Snooping on an interface, use the **show dhcpv6-snooping interface** command in privileged or global configuration mode.

show dhcpv6-snooping interace [**ethernet** | **gpon**] [*interface-id*]

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Usage Guidelines

This command displays the DHCPv6 Snooping enabled state, information on the trusted port, the number of DHCPv6 clients allowed on the physical port, and the number of currently connected DHCPv6 clients.

Example

```
Device#show dhcpv6-snooping interface
Config information of DHCPv6 Snooping:
DHCPv6 Snooping status:Enable
DHCPv6 Snooping port-down-action fast-remove:Enable
Port information:
Port          mode      maxclients    clients(ack)  clients(unack)
g0/1          untrust   2048          0             0
g0/2          untrust   2048          0             0
g0/3          untrust   2048          0             0
g0/4          untrust   2048          0             0
g0/5          untrust   2048          0             0
g0/6          untrust   2048          0             0
g0/7          untrust   2048          0             0
g0/8          untrust   2048          0             0
e1/1          untrust   2048          0             0
e1/2          untrust   2048          0             0
e1/3          untrust   2048          0             0
e1/4          untrust   2048          0             0
e2/1          untrust   2048          0             0
e2/2          untrust   2048          0             0
```

show dhcpv6-snooping vlan

To display the details of DHCPv6 Snooping on a VLAN, use the **show dhcpv6-snooping vlan** command in privileged or global configuration mode.

show dhcpv6-snooping vlan *vlan_id*

Command Default None

Command Modes Global Configuration (config)

Usage Guidelines This command displays the DHCPv6 Snooping enabled state, information on the trusted port, the number of DHCPv6 clients allowed on the physical port, and the number of currently connected DHCPv6 clients.

Example

```
Device#show dhcpv6-snooping vlan 1
Config information of DHCPv6 Snooping:
DHCPv6 Snooping status:Enable
DHCPv6 Snooping port-down-action fast-remove:Enable
Port information:
Port          mode      maxclients    clients(ack)  clients(unack)
g0/1          untrust   2048          0             0
g0/2          untrust   2048          0             0
g0/3          untrust   2048          0             0
g0/4          untrust   2048          0             0
g0/5          untrust   2048          0             0
g0/6          untrust   2048          0             0
g0/7          untrust   2048          0             0
g0/8          untrust   2048          0             0
e1/1          untrust   2048          0             0
e1/2          untrust   2048          0             0
e1/3          untrust   2048          0             0
e1/4          untrust   2048          0             0
e2/1          untrust   2048          0             0
e2/2          untrust   2048          0             0
```

show dlf-forward

To display the DLF forwarding configuration for a port, use the **show dlf-forward** command in the EXEC mode.

show dlf-forward interface { **ethernet** *port-number* | **gpon** *port-number* }

Syntax Description

ethernet *port-number*	Displays the DLF Forwarding configuration for the ethernet port.
gpon *port-number*	Displays the DLF Forwarding configuration for the gpon port.

Command Default

None

Command Modes

User EXEC
Priveleged EXEC

Examples

The following example shows how to display the DLF forwarding configuration for an ethernet port

```
Device# show dlf-forward interface ethernet 1/1
Forwarding unknown unicast packets global status:  disable
Forwarding unknown multicast packets global status:  disable
Port      Forwarding Unknown Unicast      Forwarding Unknown Multicast
e1/1      disable                         disable
```

Examples

The following example shows how to display the DLF forwarding configuration for a GPON port

```
Device# show dlf-forward interface gpon 0/1
Forwarding unknown unicast packets global status:  disable
Forwarding unknown multicast packets global status:  disable
Port      Forwarding Unknown Unicast      Forwarding Unknown Multicast
g0/1      disable                         disable
```

show ip interface

To display the IP interface configuration for the Layer 3 device, use the **show ip interface** command in the EXEC mode.

show ip interface {**loopback-interface** *loopback-interface-number* | **vlan-interface** *vlan-interface-number* | **meth-interface***meth-interface-number*}

Syntax Description

loopback-interface-number	Displays information for the loopback interface.
vlan-interface-number	Displays information for the VLAN interface.
meth-interface-number	Displays information for the meth interface.

Command Default

None

Command Modes

User EXEC
Priveleged EXEC

Examples

The followng example shows a sample output of a loopback interface:

```
Device# show ip interface loopback-interface 1
Show informations of interface
The mac-address of interface is 00:0a:5a:9b:18:15
Interface name      : LOOPBACK-IF1
Primary ipaddress   : None
Secondary ipaddress : None
Interface status    : Up


Total entries: 1 interface.
```

The followng example shows a sample output of a VLAN interface:

```
Device# show ip interface vlan-interface 1
Show informations of interface
The mac-address of interface is 00:0a:5a:9b:18:15
Interface description : interface1
Interface name        : VLAN-IF1
Primary ipaddress     : None
Secondary ipaddress   : None
VLAN                  : 1
Address-range         : 192.0.2.254-192.0.2.255,
Interface status      : Up


Total entries: 1 interface.
```

show ip source guard

To display the status and port filter applied on each port, use the **show ip-source-guard** command in privileged or global configuration mode.

```
show ip-source-guard [bind | permit | vlan]
```

Syntax Description

bind	Displays the entries of the static IP source binding table.
permit	Displays the whether Internet Group Management Protocol (IGMP) packets are permitted or not.
vlan ip *ip-address*	Displays VLAN information.

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Example

```
Device#show ip-source-guard
Port     Status   FilterType
g0/1     disable  N/A
g0/2     disable  N/A
g0/3     disable  N/A
g0/4     disable  N/A
g0/5     disable  N/A
g0/6     disable  N/A
g0/7     disable  N/A
g0/8     disable  N/A
e1/1     enable   ip+mac+vlan
e1/2     disable  N/A
e1/3     disable  N/A
e1/4     disable  N/A
e2/1     disable  N/A
e2/2     disable  N/A

Total entries:14
```

The following example displays the status of port filtering on IGMP packets:

```
Device#show ip-source-guard permit igmp

 IP source guard permit igmp status:disable
```

Related Commands

Command	Description
ip-source-guard	Configures the IP source guard function on the ports of the device.

show ipv6 interface

To display the IP interface configuration for the Layer 3 device, use the **show ipv6 interface** command in the EXEC mode.

show ipv6 interface { **loopback-interface** *loopback-interface-number* | **vlan-interface** *vlan-interface-number* | **meth-interface** *meth-interface-number* }

Syntax Description

loopback-interface-number	Displays information for the loopback interface.
vlan-interface-number	Displays information for the VLAN interface.
meth-interface-number	Displays information for the meth interface.

Command Default

None

Command Modes

User EXEC
Priveleged EXEC

Examples

The following example shows a sample output of a loopback interface:

```
Device# show ipv6 interface loopback-interface 1
Show informations of interface
The mac-address of interface is 00:0a:5a:9b:18:15
Interface name      : LOOPBACK-IF1
Primary ipaddress   : None
Secondary ipaddress : None
Interface status    : Up


Total entries: 1 interface.
```

The following example shows a sample output of a VLAN interface:

```
Device# show ipv6 interface vlan-interface 1
Show informations of interface
The mac-address of interface is 00:0a:5a:9b:18:15
Interface description : interface1
Interface name        : VLAN-IF1
Primary ipaddress     : None
Secondary ipaddress   : None
VLAN                  : 1
Address-range         : 192.0.2.254-192.0.2.255,
Interface status      : Up


Total entries: 1 interface.
```

show ipv6 nd dad attempts

To display the number of times Neighbor Solicitation (NS) messages are being sent for duplicate address detection, use the **show ipv6 nd dad attempts** command in EXEC mode.

show ipv6 nd dad attempts

Syntax Description

attempts	Displays the number of times NS messages are being sent for duplicate address detection.

Command Default

None

Command Modes

User EXEC Priveleged EXEC

The following example shows a sample output of the **show ipv6 nd dad attempts** command.

```
Device#show ipv6 nd dad attempts
Global duplicate address detection times configuration is: 1
Interface specific configurations are as follows:
Interface : DAD times

Total entries:0
```

show ipv6 nd ns retrans-time

To display the interval at which the Neighbor Solicitation (NS) messages are being sent for duplicate address detection, use the **show ipv6 nd ns retrans-time** command in EXEC mode.

show ipv6 nd ns retrans-time

Syntax Description

retrans-time	Displays the interval at which the NS messages are being sent for duplicate address detection.

Command Default

None

Command Modes

User EXEC Priveleged EXEC

The following example shows a sample out of the show ipv6 nd ns retrans-time command.

```
Device#show ipv6 nd ns retrans-time
Global neighbor solicitation retransmit time configuration is: 1 s
Interface specific configurations are as follows:
Interface : Retransmit time(s)

Total entries:0
```

show ipv6 nd reachable-time

To display the reachable time configured on an interface, use the **show ipv6 nd reachable-time** command in EXEC mode. Reachable time is the time for which a neighbor is considered to be in a reachable state.

show ipv6 nd reachable-time

Syntax Description

reachable-time	Displays the reachable time configured on an interfcae.

Command Default

None.

Command Modes

User EXEC Priveleged EXEC

The following example displays a sample output for the **show ipv6 nd reachable-time** command.

```
Device#show ipv6 nd reachable-time
Global reachable time configuration is: 30 s
Interface specific configurations are as follows:
Interface : Reachable time(s)
```

show ipv6 neighbors

To display the list of IPv6 neighbors for an interface, use the **show ipv6 neighbors** command in the EXEC mode.

show ipv6 neighbors { *ipv6-address* | **all** | **dynamic** | **static** | **mac** *mac-address* | **max-learning-num** }

Syntax Description

ipv6-address	Specifies the IPv6 address of the neighbor.
all	Displays a list of all the IPv6 neighbors.
dynamic	Displays a list of all the dynamic IPv6 neighbors.
static	Displays a list of all the static IPv6 neighbors.
mac	Displays the MAC address of all the IPv6 neighbors.
max-learning-num	Displays the maximum number of neighbors the interface is allowed to learn.

Command Default

None.

Command Modes

User EXEC Priveleged EXEC

show ipv6 route

To display the IPv6 static route configuration, use the **show ipv6 route** command in the EXEC mode.

show ipv6 route [*ospf*]

Syntax Description

ospf	Displays information of the OSPF routing configuration.

Command Default

None.

Command Modes

User EXEC
Privileged EXEC

Examples

The following example shows a sample output of the **show ipv6 route** command:

```
Device# show ipv6 route
Show ip route information

INET6 route table - vr: 0, table: 254
Route flag: U - up, G - gateway, H - host, R - reject, C - clone, S - static
Destination                   Gateway                       Flags    Use   Interface
 Metric MTU
::                            link#1                        UHRS     0     lo0
 0      0
::1                           ::1                           UH       0     lo0
 0      0
FE80::%lo0/64                 link#1                        UC       0     lo0
 0      0
FE80::%sw0/64                 link#2                        UC       1067  VLAN-IF100
 0      0
FE80::%meth0/64               link#514                      UC       0     METH-IF0
 0      0
FE80::1%lo0                   link#1                        UH       0     lo0
 0      0
FE80::20A:5AFF:FE94:804C%sw0  link#1                        UH       0     lo0
 0      0
FE80::20A:5AFF:FE94:804C%meth0 link#1                        UH       0     lo0
  0      0

Total entries: 8. Printed entries: 8.
```

show mac-address-table age-time

To display the aging time of the MAC address table, use the **show mac-address-table age-time** command in the EXEC mode.

show mac-address-table age-time

Syntax Description

age-time	Displays the aging time of the MAC address table.

Command Default

None

Command Modes

User EXEC
Priveleged EXEC

Examples

The following example shows how to display the aging time for a MAC address table:

```
Device# show mac-address-table age-time

mac address table agingtime is 300 seconds.
```

show mac-address-table

To display information about the MAC address table, use the **show mac-address-table** command in the EXEC mode.

show mac-address-table {**static** | **permanent** | **dynamic**} **blackholelearning interface ethernet***interface-number* **vlan** *vlan-id*

Syntax Description

static	Displays the static MAC address table.
permanent	Displays the permanent entries in the MAC address table.
dynamic	Displays the dynamic MAC address table.
blackhole	Displays the blachole MAC address table.
learning	Displays the MAC address learning status.

Command Default

None

Command Modes

User EXEC
Priveleged EXEC

Examples

The following example shows how to display the dynamic MAC address table:

```
Device# show mac-address-table dynamic
Show ARL table information
MAC Address        VLAN ID  port  status
00:0a:5a:a7:01:34  100      g0/1  dynamic
00:0b:ab:82:2d:82  100      e1/3  dynamic
00:0c:29:07:b6:9b  100      e1/3  dynamic
00:0c:29:15:9e:10  100      e1/3  dynamic
00:0c:29:3c:3b:08  100      e1/3  dynamic
00:0c:29:3c:3b:12  100      e1/3  dynamic
00:0c:29:71:b1:4f  100      e1/3  dynamic
00:0c:29:71:b1:59  100      e1/3  dynamic
00:0c:29:b8:0f:0b  100      e1/3  dynamic
00:0c:29:b8:0f:15  100      e1/3  dynamic
00:11:32:47:9a:30  100      e1/3  dynamic
00:19:bb:2f:5a:81  100      e1/3  dynamic
00:19:bb:30:70:97  100      e1/3  dynamic
00:19:bb:30:a0:6b  100      e1/3  dynamic
00:1f:26:35:7a:9f  100      e1/3  dynamic
00:21:5a:a9:53:14  100      e1/3  dynamic
00:23:5d:fd:94:00  100      e1/3  dynamic
00:30:18:cc:7b:02  100      e1/3  dynamic
00:50:56:92:0a:09  100      e1/3  dynamic
00:50:56:92:88:2f  100      e1/3  dynamic
00:50:56:95:41:5e  100      e1/3  dynamic
00:50:56:bd:2b:cf  100      e1/3  dynamic
00:61:56:60:93:84  100      e1/3  dynamic
00:d0:0a:0b:ea:1c  100      e1/3  dynamic
00:e0:4c:86:70:01  100      e1/3  dynamic
00:eb:d5:5e:02:a0  100      e1/3  dynamic
0c:f5:a4:ba:44:9f  100      e1/3  dynamic
2c:ab:eb:22:76:8d  100      e1/3  dynamic
```

```
40:a6:e8:e6:52:de  100      e1/3  dynamic
40:a6:e8:e6:b5:5c  100      e1/3  dynamic
44:8a:5b:98:e9:60  100      e1/3  dynamic
5c:71:0d:bb:35:8b  100      e1/3  dynamic
5c:71:0d:bb:3c:19  100      e1/3  dynamic
5c:71:0d:bb:60:fa  100      e1/3  dynamic
68:9c:e2:a0:7d:3e  100      e1/3  dynamic
68:9c:e2:a0:7d:5e  100      e1/3  dynamic
68:ca:e4:3a:3d:e0  100      e1/3  dynamic
68:ef:bd:f0:d1:08  100      e1/3  dynamic
b0:7d:47:3f:47:ae  100      e1/3  dynamic
c8:f9:f9:45:12:5b  100      e1/3  dynamic
e4:1f:13:43:41:0a  100      e1/3  dynamic
e4:1f:13:77:9f:06  100      e1/3  dynamic
e4:1f:13:77:a0:c8  100      e1/3  dynamic
Total entries: 43 .
```

Examples

The following example shows how to display the static MAC address table:

```
Device# show mac-address-table static
Show ARL table information
MAC Address        VLAN ID  port  status
00:0a:5a:9b:18:15  1        cpu   static
00:0a:5a:9b:18:15  100      cpu   static
Total entries: 2 .
```

Examples

The following example shows how to display the MAC address table learning status:

```
Device# show mac-address-table learning interface ethernet 1/1
Port      Mac learning status
e1/1      enable
Total entries: 1 .
```

show mirror

To see the port mirror configuration, use the **show mirror** command in privileged or global configuration mode.

```
show mirror
```

Command Default None

Command Modes Privileged (#)

Global Configuration (config)

Example

```
Device#show mirror
Information about mirror port(s)
The monitor port            : e1/4
The mirrored egress ports   : cpu,e1/1-e1/2.
The mirrored ingress ports  : cpu,e1/1-e1/2.
```

show snmp community

To display the SNMP community strings configured on the switch, use the **show snmp community** command in privileged or global configuration mode.

```
show snmp community
```

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Example

```
Device#show snmp community
Show snmp community information
Encryption status: OFF
index  community  priority  state   view-name
1      public     ro        permit  iso
2      private    rw        permit  iso
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string

show snmp contact

To display the SNMP contact string, use the **show snmp contact** command in privileged or global configuration mode.

```
show snmp contact
```

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Example

```
Device#show snmp contact
Manager contact information : http://
```

Related Commands

Command	Description
snmp-server contact	Sets the SNMP manager contact information

show snmp engineid

To display the identification of the local SNMP engine and all remote engines that have been configured on the device, use the **show snmp engineid** command in privileged or global configuration mode.

```
show snmp engineid {local |remote }[engineid]
```

Command Default None

Command Modes Privileged (#)

Global Configuration (config)

Example

The following is a sample output of the **show snmp engineid local** command

```
Device#show snmp engineid local
Local engine id: : 134640000000000000000000
```

Related Commands

Command	Description
snmp-server engineid	Configures engine ID on the device.

show snmp group

To display the different SNMP group configurations, use the **show snmp group** command in privileged or global configuration mode.

```
show snmp group
```

Command Default None

Command Modes Privileged (#)

Global Configuration (config)

Usage Guidelines Use this command to view the names of configured SNMP groups, the security models being used, and the different views configured under each group.

Example

```
Device#show snmp group
groupname: g3
securitymodel: 3 auth
readview: iso
writeview: iso
notifyview: no specified notifyview
context: default value(NULL)

groupname: initial
securitymodel: 3 noauthpriv
readview: iso
writeview: iso
notifyview: iso
context: default value(NULL)

groupname: initial
securitymodel: 3 auth
readview: iso
writeview: iso
notifyview: iso
context: default value(NULL)


group snmp3 number:3
```

Related Commands

Command	Description
snmp-server group	Configures an SNMP group

show snmp host

To display the recipient details for the SNMP trap notifications, use the **show snmp host** command in privileged or global configuration mode.

```
show snmp host
```

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Example

```
Device#show snmp host
Show SNMP trap host information
SNMP host ip  security  version
10.75.166.19  public    2c
```

Related Commands

Command	Description
snmp-server host	Configures the recipient for the SNMP notifications.

show snmp location

To display the SNMP manager location string, use the **show snmp location** command in privileged or global configuration mode.

```
show snmp location
```

Command Default None

Command Modes Privileged (#)

Global Configuration (config)

Example

```
Device#show snmp location
Switch location information : sample sysLocation factory default
```

Related Commands

Command	Description
snmp-server location	Sets the SNMP manager location string.

show snmp mib

To display the Management Information Base (MIB) module instance identifiers, use the **show snmp mib** command in privileged or global configuration mode.

```
show snmp mib [module module-name]
```

Syntax Description

module *module-name*	Specifies the MIB module object instance identifier

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Usage Guidelines

SNMP MIB is a repository for information about device parameters and network data. Collections of related objects are defined in MIB modules.

The **show snmp mib** command displays the instance identifiers for all the MIB objects on the system. The MIB module table names are registered when the system initializes.

Note The **show snmp mib** command generates a high volume of output if SNMP is enabled on your system.

Example

The following is a sample output that shows the details of the **gbnL2PppoePlus** MIB module:

```
Device#show snmp mib module gbnL2PppoePlus

gbnL2PppoePlus:pppoeplusType-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.2.0]
gbnL2PppoePlus:pppoeplusFormat-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.3.0]
gbnL2PppoePlus:pppoeplusDelimiter-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.4.0]
gbnL2PppoePlus:pppoeplusCircuitidOrder-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.5.0]
gbnL2PppoePlus:pppoeplusCircuitidString-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.6.0]
gbnL2PppoePlus:pppoeplusRemoteidOrder-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.7.0]
gbnL2PppoePlus:pppoeplusRemoteidString-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.8.0]
gbnL2PppoePlus:pppoeplusPortsIndex-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.9.1.1.1]
gbnL2PppoePlus:pppoeplusPortsOnOff-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.9.1.2.1]
gbnL2PppoePlus:pppoeplusPortsTrust-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.9.1.3.1]
gbnL2PppoePlus:pppoeplusPortsDropPadi-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.9.1.4.1]
gbnL2PppoePlus:pppoeplusPortsDropPado-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.9.1.5.1]
gbnL2PppoePlus:pppoeplusPortsStrategy-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.9.1.6.1]
gbnL2PppoePlus:pppoeplusPortsCircuit-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.9.1.7.1]
```

show snmp name

To display the SNMP system name, use the **show snmp name** command in privileged or global configuration mode.

```
show snmp name
```

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Example

```
Device#show snmp name
system name : 2
```

Related Commands

Command	Description
snmp-server name	Sets the SNMP system name.

show snmp notify

To display the configured SNMP notifications on the system, use the **show snmp notify** command in privileged or global configuration mode.

```
show snmp notify
```

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Example

```
Device#show snmp notify
Name         Type  State
bridge       trap  enabled
gbn          trap  enabled
gbnsavecfg   trap  enabled
interfaces   trap  enabled
rmon         trap  enabled
snmp         trap  enabled
if-ethernet     Link-Trap
g0/1            enabled
g0/2            enabled
g0/3            enabled
g0/4            enabled
g0/5            enabled
g0/6            enabled
g0/7            enabled
g0/8            enabled
e1/1            enabled
e1/2            enabled
e1/3            enabled
e1/4            enabled
e2/1            enabled
e2/2            enabled
```

Related Commands

Command	Description
snmp-server trap-source	Configures an the interface that originates SNMP traps.
snmp-server enable	Enables SNMP notifications

show snmp user

To display information about the configured SNMP users, use the **show snmp user** command in privileged or global configuration mode.

```
show snmp user
```

Command Default None

Command Modes Privileged (#)

Global Configuration (config)

Example

```
Device#show snmp user
User name: u3
Engine ID: 134640000000000000000000
Authentication Protocol: HMACMD5AuthProtocol
Group-name: g3
Validation: valid

User name: initialmd5
Engine ID: 134640000000000000000000
Authentication Protocol: HMACMD5AuthProtocol
Group-name: initial
Validation: valid

User name: initialsha
Engine ID: 134640000000000000000000
Authentication Protocol: HMACSHAAuthProtocol
Group-name: initial
Validation: valid

User name: initialnone
Engine ID: 134640000000000000000000
Authentication Protocol: NoauthProtocol
Group-name: initial
Validation: valid

user number:4
```

Related Commands

Command	Description
snmp-server user	Configures an SNMP user in a group.

show snmp view

To display the details of an SNMP view, use the **show snmp view** command in privileged or global configuration mode.

```
show snmp view[view-name]
```

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Example

```
Device#show snmp view
View Name  Type     Subtree
iso        Include  1
sysview    Include  1.3.6.1.2.1.1
internet   Include  1.3.6.1

view number:3
```

Related Commands

Command	Description
snmp-server view	Configures an SNMP view

shutdown

To shut down a VLAN interface, use the **shutdown** command in the VLAN configuration mode. You can cancel the shuydown of the VLAN interface by using the **no** form of the command.

shutdown

no shutdown

Syntax Description

shutdown	Shuts down the VLAN interface.

Command Default

None

Command Modes

VLAN configuration

Examples

The following example shows how to shut down a VLAN interface:

```
Device(config-if-vlanif)# shutdown
```

snmp-server

To enable or disable Simple Network Management Protocol (SNMP) on a device use the **snmp-server** command in the global configuration mode.

```
snmp-server {enable [informs |traps][bridge | gbn | gbnsavecfg | interfaces
| rmon | snmp]] | disable}
```

Syntax Description

enable	Enables SNMP traps on the device
disable	Disables the SNMP server
informs	Configures SNMP inform request
traps	Configures SNMP trap notifications

- **bridge** Specifies the type of SNMP informs or traps notifications to be enabled.
- **gbn** If you do not specify the type of SNMP inform or trap, all traps and informs that are configured on your system are enabled.
- **gbnsavecfg**
- **interfaces**
- **rmon**
- **snmp**

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

The **snmp-server enable** command is optional. SNMP traps and informs are enabled by default, on the device. Use the **snmp-server disable** command to disable SNMP traps or informs on the device.

Example

```
Device#configure terminal
Device(config)#snmp-server enable traps gbn
```

snmp-server community

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP) use the **snmp-server community** command in the global configuration mode. To remove the configured community string, use the **no** form of the command.

```
[no] snmp-server community  {name|md5 }{ro|rw}{deny|permit}[view view-name]
```

Syntax Description

name	SNMP community name that consists of 1 to 32 characters
md5	Uses md5 for authentication
ro	Specifies read-only access. Authorized management stations can retrieve only MIB objects
rw	Specifies read-write access. Authorized management stations can both retrieve and modify MIB objects.
permit	Specifies community name string is active
deny	Specifies community name string is not activated
view *view-name*	(Optional) Specifies a previously defined view. The view defines the objects available to the SNMP community. Default view is ISO.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

The SNMP community name authenticates access to MIB objects. In order for the NMS to access the switch, the community name definitions on the NMS must match at least one of the community name definitions on the switch.

Examples

The following example shows how to set the read/write community string to group1:

```
Device#configure terminal
Device(config)#snmp-server community group1 rw permit
```

The following example shows how to assign the string manager to SNMP and allow read-only access to the objects in the view called restricted:

```
Device(config)#snmp-server community group1 ro permit view restricted
```

The following example shows how to remove the community 1:

```
Device(config)#no snmp-server community 1
```

snmp-server community encrypt

To enable or disable encryption of community access string, use the **snmp-server community encrypt** command in the global configuration mode.

```
snmp-server community encrypt  {enable|disable }
```

Syntax Description

enable	Enables encryption of the community name string
disable	Disables encryption of community name string

Command Default

The community name string is not encrypted.

Command Modes

Global configuration (config)

Example

```
Device#configure terminal
Device(config)#snmp-server community encrypt enable
```

snmp-server contact

To configure the SNMP manager contact information, use the **snmp-server contact** command in the global configuration mode. To remove the SNMP manager contact information, use the **no** form of the command.

`snmp-server contact` *contact-information*

Syntax Description

contact-information	Specifies the SNMP manager contact details

Command Default

SNMP manager contact string is not set.

Command Modes

Global Configuration (config)

Example

```
Device(config)#snmp-server contact SystemOperator
```

snmp-server encrypt

To enable or disable the encryption of the password for a user, use the **snmp-server encrypt** command in the global configuration mode.

A password is encrypted by default.

```
snmp-server encrypt {enable|disable}
```

Syntax Description

enable	Enables the encryption of password
disable	Disables the encryption of password

Command Default

None

Command Modes

Global configuration (config)

Example

```
Device#configure terminal
Device(config)#snmp-server encrypt disable
```

snmp-server engineid

To configure the Simple Network Management Protocol (SNMP) engine ID on a local device or a remote device, use the **snmp-server** command in the global configuration mode.

`snmp-server engineid local` *engineid* `|` `remote` *ip-address* `[udp-port`*port-num*`]` *engineid*

Syntax Description

local *engineid*	Specifies the engine ID of the local device
remote *ip-address*	Specifies the engine ID of the local device
udp-port*port-num*	Specifies the UDP port on the remote device

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

An SNMP engine ID is a unique string that identifies the device, for administrative purposes.

The engine ID of the local SNMP device is 134640000000000000000000. You can modify the local engine ID, but not delete it. You can create and delete the engine ID of a remote SNMP device. If you delete a remote engine ID, the corresponding users are also deleted. You can configure a maximum number of 32 remote engine IDs.

Example

```
Device#configure terminal
Device(config)#snmp-server engineid remote 172.16.20.4 1
```

snmp-server group

To configure an SNMP group that enables authentication for the members of a specified view, use the **snmp-server group** command in the global configuration mode. To remove the configured authentication for the SNMP group, use the **no** form of the command.

`[no] snmp-server group` *group-name*`3 [auth |noauthpriv |priv] read` *read-view* `write` *write-view* `notify` *notify-view*

Syntax Description

auth	Specifies that packets are authenticated but not encrypted.
noauthpriv	Specifies that packets are not authenticated.
priv	Specifies that packets are authenticated and not encrypted.
read *read-view*	(Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent. If a *read-view* is not specified, it defaults to the iso view and auth security level.
write *write-view*	(Optional) Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent. **write-view** does not have defaults. Hence it is mandatory to specify it if **write** is configured.
notify *notify-view*	(Optional) Specifies a notify view for the SNMP group. This view enables you to specify a notification or a trap. **notify-view** does not have defaults. Hence it is mandatory to specify *notify-view* if **notify** is configured.

Command Default

None

Command Modes

Global configuration (config)

Examples

```
Device#configure terminal
Device(config)#snmp-server group g1 3 priv write dept-view
```

snmp-server host

To configure the recipient of an SNMP notification operation, use the **snmp-server host** command in the global configuration mode. To remove the configured recipient for the SNMP group, use the **no** form of the command.

```
[no] snmp-server host {inet6 ipv6-address |ipv4-address}{version {1 | 2c | 3{auth
| noauthpriv | priv }} }security-name [udp-port udp-port-num][ notify-type[bridge
| gbn | gbnsavecfg | interfaces | rmon | snmp] ]
```

Syntax Description

inet6 *ipv6-address*	Specifies the IPv6 address of the recipient of SNMP traps
ipv4-address	Specifies the IPv4 address of the recipient of SNMP traps
version {**1** | **2c** | **3**{**auth** | **noauthpriv** | **priv** }	Specifies the SNMP version: 1, 2c, 3. If you specify SNMP version 3, ensure that you specify the security levels too: • **auth**: Enables MD5 and SHA packet authentication • **noauth**: Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3. • **priv**: Enables Data Encryption Standard (DES) packet encryption.
security-name	Defines a name for this configuration.
udp-port *udp-port-num*	Specifies the UDP port on the host device.
notify-type	Specifies the type of notification to be sent to the host: • bridge • gbn • gbnsavecfg • interfaces • rmon • snmp

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

Use the **snmp-server host** command to configure a recipient for the SNMP notifications. If this command is not configured, no notifications are sent. **snmp-server host** command is used in conjunction with the **snmp-server enable** command. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

Examples

```
Device#configure terminal
Device(config)#snmp-server host 192.168.5.1 version 2c test-sec udp-port 4
```

snmp-server location

To set the SNMP server location string, use the **snmp-server location** command in the global configuration mode. To remove the SNMP server location information, use the **no** form of the command.

```
[no] snmp-server location syslocation
```

Syntax Description

syslocation	String that describes the SNMP server location

Command Default

No system location string is set.

Command Modes

Global Configuration (config)

Example

```
Device(config)#snmp-server location Building13
```

snmp-server max-packet-length

To configure the maximum size of SNMP packets, use the **snmp-server max-packet-length** command in the global configuration mode. To remove the maximum packet length configuration for SNMP packets, use the **no** form of the command.

```
[no] snmp-server max-packet-length length
```

Syntax Description

length	Specifies the maximum packet length for SNMP packets. The value ranges from 484 bytes through 8000 bytes. Default value is 1000 bytes.

Command Default

Maximum packet length is set to 1000 bytes.

Command Modes

Global Configuration (config)

Example

```
Device(config)#snmp-server max-packet-length 1200
```

snmp-server name

To set the SNMP system name string, use the **snmp-server name** command in the global configuration mode. To remove the SNMP server name information, use the **no** form of the command.

```
[no] snmp-server name sysname
```

Syntax Description

sysname	String that describes the SNMP server name

Command Default

No system name string is set.

Command Modes

Global Configuration (config)

Example

```
Device(config)#snmp-server name Building13Server
```

snmp-server trap-source

To specify the interface from which the Simple Network Management Protocol (SNMP) trap should originate, use the **snmp-server trap-source** command in the global configuration mode. To remove the source of SNMP trap, use the **no** form of the command.

`snmp-server trap-source {inet6 |vlan-interface` *vlan-id*`|loopback-interface` *interface*`|vlan-interface` *vlan-id*`}`

Syntax Description

inet6	Specifies the IPv6 address family
vlan-interface *vlan-id*	Specifies the VLAN id to which the VLAN interfaces that originate the traps, belong.
loopback-interface *interface*	Specifies the loopback interface that is configured as the origin of the traps.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

Use this command to monitor notifications from a particular interface.

An SNMP trap or inform that is sent from an SNMP server has a notification address of the interface it went out of at that time.

Example

```
Device#configure terminal
Device(config)#snmp-server trap-source vlan-interface 3
```

snmp-server user

To configure a new user to an SNMP group, use the **snmp-server user** command in the global configuration mode. To remove a configured user from an SNMP group, use the **no** form of this command.

`[no]snmp-server user` *username group-name* `[remote` *ipaddress* `[udp-port` *port-number* `] ] [auth {md5 |sha }{auth-password {authpassword |encrypt-authpassword` *password*`} |auth-key{`*authkey* `| encrypt-authkey`*password*`}}[privdes {priv-key{`*key*`| encrypt-privkey`*key*`}| priv-password{`*password* `| encrypt-privpassword`*privpassword*`} } ] ]`

Syntax Description

username	Name of the user created
group-name	Name of the SNMP group to which the user belongs
remote	(Optional) A remote SNMP entity to which the user belongs
ipaddress	(Optional) IP address of the remote SNMP host.
udp-port *port-number*	(Optional) UDP port on the remote port
auth	(Optional) Specifies which authentication level should be used.
md5	(Optional) Specifies the HMAC-MD5-96 authentication level
sha	(Optional) Specifies the HMAC-SHA-96 authentication level
auth-password *authpassword*	Specifies the authentication password
auth-key *authkey*	Specifies the authentication key
priv	(Optional) Specifies the use of the User-based Security Model (USM) for SNMP version 3 for SNMP message level security.
des	(Optional) Specifies the use of the 56-bit Digital Encryption Standard (DES) algorithm for encryption.
priv-key	(Optional) String that specifies the privacy user password.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

The **snmp-server user** command configures a user for a local engine or a remote engine.

The following three users exist by default and they are reserved as the system users:

- initialmd5
- initialsha
- initialnone

To configure a remote engine user, specify remote ipaddress. If you do not specify remote ipaddress, a local engine user is configured.

For a remote user, the default port number is 162. To configure a different remote port, specify a udp-port port-number .

Three levels of user privileges can be specified:

- **noauthpriv** : Authentication and password encryption are not required. It is the default configuration.
- **auth**: Authentication is required but password encryption is not required.
- **authpriv**: Authentication and password encryption, both are required.

Note The user security level should be the same as the corresponding group security level.

Example

```
Device#configure terminal
Device(config)#snmp-server user u3 g3 auth md5 auth-password password1
```

snmp-server view

To create or update an SNMP server view, use the **snmp-server view** command in the global configuration mode. To remove the configured SNMP server view, use the **no** form of the command.

```
[no] snmp-server view view-name oid-subtree {include | exclude}
```

Syntax Description

oid-subtree	Object identifier (OID) of the ASN.1 subtree that is either included or excluded from the view. A string that can have upto to 64 characters.
view-name	Name of the SNMP view that is to be created.
exclude	Excludes the OID specified in the *oid-subtree* argument from the SNMP view.
include	Includes the OID specified in the *oid-subtree* argument in the SNMP view.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

Use this command to create a view that is a list of SNMP object trees, which you can access. The **iso**, **internet** and **sysview** views exist by default. You cannot delete or modify the **internet** view.

Examples

The following example creates a view named **oneview** and excludes all objects of the subtree:

```
Device#configure terminal
Device(config)#snmp-server view oneview 1.3 exclude
```

PART VI

Quality of Service

Quality of Service

bandwidth egress rate

To set the bandwidth limit on the outbound traffic on a port, use the **bandwidth egress** *rate* command in the interface configuration mode. To remove the configured bandwidth limit, use the **no** form of the command.

```
[no]bandwidth egress target-rate [ target-burst-rate ]
```

Syntax Description

target-rate	Specifies the bandwidth limit in Kbps. The target rate must be a multiple of 64K and should range between 2048 and 2608832 Kbps: It should be 2048 to 1024000 Kbps for a GE port, 2048 to 2608832 Kbps for a PON port, and 2048 to 10240000 for a 10GE port.
target-burst-rate	Specifies the burst transmission rate. Target burst rate (Kbps) must be a multiple of 64K Values can range between 2048 through 2608832.

Command Default

None

Command Modes

Interface Configuration (config-if)

Example

```
Device#configure terminal
Device(config)#interface e1/1

Device(config-if-ethernet-1/1)#bandwidth egress 2048
```

clear traffic-statistic

To remove the traffic statistics records, use the **clear traffic-statistic** command in the global configuration mode.

clear traffic-statistic { [**all** | [**ip-group** {**num** | **name** } [**subitem** *subitem*]] [**link-group** {**num** | **name** } [**subitem** *subitem*]]] }

ip-group {**num**	**name** }	Specifies a standard or extended ACL.
link-group {**num**	**name** }	Specifies a Layer 2 ACL.
subitem *subitem*	Specifies the sub item in the ACL.

Command Modes

Global Configuration (config)

Command Default

None

Usage Guidelines

Use the **clear traffic-statistic all** command to remove all traffic statistics records.

Use the **clear traffic-statistic ip-group** or **clear traffic-statistic link-group** command to remove the traffic statistics records that are generated for the specified access control list.

Example

```
Device#configure terminal
Device(config)#clear traffic-statistic ip-group 3
```

queue-scheduler cos-map

To map the 802.1p priorities to the hardware queue, use the **queue-scheduler cos-map** command in the global configuration mode. To restore the default queue scheduler settings, use the **no** form of the command.

```
[no ]queue-scheduler cos-map [queue-class] [priority]
```

Syntax Description

queue-class	Specifies the hardware queue value which ranges from 0 through 7.
priority	Specifies the 802.1p priority. The value ranges from 0 to 7.

Command Default

Strict Priority scheduling is followed by default.

Command Modes

Global configuration (config)

Usage Guidelines

802.1p is used to classify the outgoing traffic at the egress port based on the 802.1p priority. For each message that enters the switch, the system maps the specific hardware queue priority according to the 802.1p priority of the message.

Changing the mapping relation between 802.1p priority and hardware queues changes the mapping relation between 802.1p priorities and output queues.

If two 802.1p priorities are mapped to the same hardware priority queue, messages of the two 802.1p priorities cannot be forwarded with 1:1 forwarding.

Use the **queue-scheduler cos-map** command to set the 802.1p mapping with hardware queue priority.

Example

The following example shows how to map packets with priority 0 to queue 1:

```
Device#configure terminal
Device(config)#queue-scheduler cos-map 1 0
Config successfully.
```

queue-scheduler strict-priority

To configure the strict priority queue scheduling algorithm on the queue scheduler, use the **queue-scheduler strict-priority** command in the global configuration mode. To restore the default queue scheduler settings, use the **no** form of the command.

```
[no ]queue-scheduler strict-priority
```

Command Default

Strict Priority scheduling is followed by default.

Command Modes

Global configuration (config)

Usage Guidelines

Strict-Priority Queuing is designed for critical business applications wherein the services are prioritized in order to reduce the latency of response when a congestion occurs. The priority queue classifies all messages into eight class: 7,6,5,4,3,2,1, and 0, in the order of priority. The group of critical services is put into the higher priority queue and non-critical business group is put into the lower priority queue. The higher priority queue is first emptied before the messages in the lower priority queue are sent. Messages in the group of non-critical business are transmitted in the idle gap of handling critical business data.

Example

```
Device#configure terminal
Device(config)#queue-scheduler strict-priority
```

queue-scheduler sp-wrr

To configure strict priority and weighted round robin (WRR) queue scheduling algorithm on the queue scheduler, use the **queue-scheduler sp-wrr** command in the global configuration mode. To restore the default queue scheduler settings, use the **no** form of the command.

```
[no ]queue-scheduler sp-wrr {w1| w2| w3| w4| w5| w6| w7| w8}
```

Syntax Description

wx	Specifies the weight of the queue represented by x.
where x can be 1, 2, 3, 4, 5, 6, 7,8	For example, w1 represents the weight of the first queue. w2 represents the weight of the second queue.

Command Default

Strict Priority scheduling is followed by default.

Command Modes

Global configuration (config)

Usage Guidelines

Strict-Priority and WRR queue scheduling combines the algorithms of strict-priority and Weighted round robin scheduling. If the weight of the queue is set to 0, the queue follows the Strict-Priority queuing algorithm to send messages. A non-zero value of the weight puts the queue to the WRR scheduling mechanism.

Example

```
Device#configure terminal
Device(config)#queue-scheduler sp-wrr 1 2 3 4 5 6 7 8
```

queue-scheduler wrr

To configure the weighted round robin (WRR) queue scheduling algorithm on the queue scheduler, use the **queue-scheduler wrr** command in the global configuration mode. To restore the default queue scheduler settings, use the **no** form of the command.

```
[no ]queue-scheduler wrr{ w1| w2| w3| w4| w5| w6| w7| w8}
```

Syntax Description

wx	Specifies the weight of the queue represented by x.
where x can be 1, 2, 3, 4, 5, 6, 7,8	For example, w1 represents the weight of the first queue. w2 represents the weight of the second queue.

Command Default

Strict Priority scheduling is followed by default.

Command Modes

Global configuration (config)

Usage Guidelines

Weighted Round Robin (WRR) queue scheduling divides each port into eight output queues: 7, 6, 5, 4, 3, 2, 1, and 0, in the that order of priority, with 7 being the highest priority. All the queues are scheduled by turns and each queue gets a certain service time. Each queue of WRR can be configured with weighted values of w7, w6, w5, w4, w3, w2, w1, or w0. The weighted value represents the weight of the resource.

An advantage of WRR queuing is that although multiple queues are scheduled by polling, each queue is not assigned a fixed time slot. If a queue is empty, it immediately switches to the next queue schedule. So, the bandwidth and resources of that queue can be fully utilized

Example

```
Device#configure terminal
Device(config)#queue-scheduler wrr 1 2 3 4 5 6 7 8
```

queue-scheduler dscp-map

To configure the strict priority queue scheduling algorithm on the queue scheduler, use the **queue-scheduler dscp-map** command in the global configuration mode. To restore the default queue scheduler settings, use the **no** form of the command.

```
[no ]queue-scheduler dscp-map [dscp-value] [priority]
```

Syntax Description

dscp-value	Specifies the DSCP value whioch ranges from 0 through 63.
priority	Specifies the 802.1p priority. The value ranges from 0 to 7.

Command Default

Strict Priority scheduling is followed by default.

Command Modes

Global configuration (config)

Usage Guidelines

DSCP mapping is disable by default. To enable DSCP mapping use the **queue-scheduler dscp-map** command.

DSCP allows 64 priority values whereas 802.1p (hardware queue) allows only eight priority values. By default, the following is the mapping between DSCP and 802.1p:

DSCP	802.1p
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48055	6
56-63	7

Example

The following example shoes how to map DSCP 56 to 802.1p priority 6:

```
Device#configure terminal
Device(config)#queue-scheduler dscp-map

Device(config)#queue-scheduler dscp-map 56 6
```

rate-limit

To set the traffic rate limit in inbound or outbound direction, use the **rate-limit** command in the global configuration mode. To remove the rate limit, use the **no** form of the command.

[**no**] **rate-limit** {**input** | **output** } { [**ip-group** {**num** | **name** } [**subitem** *subitem*]] [**link-group** {**num** | **name** } [**subitem** *subitem*]] } *target-rate*

input	Specifies the rate limit in inbound direction.
output	Specifies the rate limit in outbound direction.
ip-group {**num**	**name** }	Specifies a standard or extended ACL.
link-group {**num**	**name** }	Specifies a Layer 2 ACL.
subitem *subitem*	Specifies the sub item in the ACL.
target-rate	Specifies target rate which is the traffic rate limit in Kbps. Target rate should be a multiple of 64, and can range from 64 to 1048512.

Command Modes Global Configuration (config)

Command Default None

Usage Guidelines Use the **rate-limit input** command to limit the traffic rate in the inbound direction.

Use the **rate-limit output** command to limit the traffic rate in the outbound direction.

Use this command to monitor the rate of traffic that enters a device. If the traffic exceeds a certain threshold, you can define policies to take suitable measures.

Example

The following example sets the inbound traffic rate limit to 100 Kbps:

```
Device#configure terminal
Device(config)#rate-limit input ip-group 3 100
```

show bandwidth egress

To display the rate limit and the burst rate that are set for the egress interface, use the **show bandwidth egress** command in privileged or global configuration mode.

```
show bandwidth egress[ interface {ethernet | gpon }port-num]
```

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Example

The following is a sample output of the **show bandwidth** command.

```
Device(config)#show bandwidth egress
g0/1: bandwidth egress
  limit rate:  / Kbps     burst:   / Kbps

g0/2: bandwidth egress
  limit rate:  / Kbps     burst:   / Kbps

g0/3: bandwidth egress
  limit rate:  / Kbps     burst:   / Kbps
 ....
 ...
e2/2: bandwidth egress
  limit rate:  / Kbps     burst:   / Kbps
```

Related Commands

Command	Description
bandwidth egress rate	Sets the bandwidth limit on the outbound traffic on a port.

show qos-info all

To display the parameters that are set for Quality of Service (QoS), use the **show qos-info** command in privileged or global configuration mode.

```
show qos-info {all| traffic-copy-to-cpu | mirrored-to | traffic-priority
| traffic-redirect | traffic-statistic| statistic }
```

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Usage Guidelines

Use the **show qos-info all** command to display all the configured QoS parameters.

Use the **show qos-info statistic** command to display all the statistics for QoS parameters.

Use the **show qos-info traffic-copy-to-cpu** command to display the parameter settings for copying messages to the CPU.

Use the **show qos-info mirrored-to** command to display the parameter settings for traffic mirroring.

Use the **show qos-info traffic-priority** command to display the parameter settings for traffic priority.

Use the **show qos-info traffic-redirect** command to display the parameter settings for message redirection.

Example

```
Device#show qos-info all
mirrored-to(max 3 dest port):
traffic-priority:
traffic-redirect:
traffic-statistic:
traffic-copy-to-cpu:
```

Here is a sample ouput for the **show qos-info statistic** command:

```
Device#show qos-info statistic
mirrored-to:
total mirrored-to rules         : 0 rules

traffic-priority:
total traffic-priority rules    : 0 rules

traffic-redirect:
total traffic-redirect rules    : 0 rules

traffic-statistic:
total traffic-statistic rules   : 0 rules

traffic-copy-to-cpu:
total traffic-copy-to-cpu rules : 0 rules

total mirrored-to rules         : 0 rules
total traffic-priority rules    : 0 rules
```

```
total traffic-redirect rules    : 0 rules
total traffic-statistic rules   : 0 rules
total traffic-copy-to-cpu rules : 0 rules
total qos-info rules            : 0 rules
```

Related Commands

Command	Description
traffic-copy-to-cpu	Copies all packets to the CPU.
traffic-statistic	Configures the system to collect the traffic statistics
traffic-redirect	Redirects the traffic to a specified interface or to the CPU.

show qos-interface

To display all the policies set for Quality of Service (QoS) on the interface, use the **show qos-interface** command in privileged or global configuration mode.

```
show qos-interface {all| rate-limit | statistic
```

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Usage Guidelines

Use the **show qos-interface all** command to display all the QoS parameters for the interface.

Use the **show qos-interface rate-limit** command to display the rate limit parameters for the interface.

Use the **show qos-interface statistic** command to display the statistics of rate limit for all interfaces.

Example

The following is a sample output of the **show qos-interface all** command:

```
Device#show qos-interface all
total qos-interface rules : 0 rules
```

The following is a sample output of the **show qos-interface rate-limit** command:

```
Device#show qos-interface rate-limit
total rate-limit rules : 0 rules
```

The following is a sample output of the **show qos-interface statistic** command:

```
Device#show qos-interface satistic
total qos-interface rules : 0 rules
```

show queue-scheduler

To display information about the queue scheduler, use the **show queue-scheduler** command in privileged or global configuration mode.

```
show queue-scheduler [ cos-map | dscp-map ]
```

Syntax Description

cos-map	Specifies the 802.1p and hardware queue mapping.
dscp-map	Specifies the DSCP and 802.1p value mapping.

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Usage Guidelines

Use the **show queue-scheduler** command to display information about the queue scheduler parameters.

Use the **show queue-scheduler cos-map** command to display information about the mapping between 802.1p and hardware.

Use the **show queue-scheduler dscp-map** command to display information about the mapping between 802.1p values and DSCP.

Examples

Following are sample outputs for the **show queue-scheduler** commands.

```
Device#show queue-scheduler
Queue scheduler status : enable
Queue scheduler mode   : SP (Strict Priority)
```

```
Device#show queue-scheduler cos-map
Information about map of cos:
802.1P Priority  Queue of class
--------------------------------
0                0
1                1
2                2
3                3
4                4
5                5
6                6
7                7
```

```
Device#show queue-scheduler dscp-map
dscp-pri has been disabled.
```

Related Commands

Command	Description
queue-scheduler wrr	Configures the weighted round robin scheduling mode.

Command	Description
queue-scheduler strict-priority	Configures the strict priority scheduling mode.
queue-scheduler dscp-map	Maps DSCP values to hardware priority values.
queue-scheduler cos-map	Maps 802.1p values to hardware queue map.

storm-control

To enable traffic storm control on an interface and to configure a threshold for the number of packets on the port, use the**storm-control** command in the interface configuration mode. To remove the storm control configuration on an interface, use the **no** form of the command.

```
[no]storm-control {broadcast | multicast | unicast } target-rate
```

Syntax Description

broadcast	Specifies broadcast traffic for storm control.
multicast	Specifies multicast traffic for storm control.
unicast	Specifies unicast traffic for storm control.
target-rate	Specifies a threshold limit for the number of packets on the port. Value can range from 64 to 32000000 packets per second (pps) Default value is 49984 pps

Command Default

None

Command Modes

Interface Configuration (config-if)

Example

```
Device#configure terminal
Device(config)#interface e1/1

Device(config-if-ethernet-1/1)#storm-control unicast 512
Device(config-if-ethernet-1/1)#storm-control multicast 256
Device(config-if-ethernet-1/1)#storm-control broadcast 128
```

traffic-copy-to-cpu

To copy the packets that match an ACL to CPU, use the **traffic-copy-to-cpu** command in the global configuration mode. To remove the traffic copy configuration, use the **no** form of the command.

[**no**] **traffic-copy-to-cpu** { [**ip-group** {**num** | **name** } [**subitem** *subitem*]] [**link-group** {**num** | **name** } [**subitem** *subitem*]] }

ip-group {**num**	**name** }	Specifies a standard or extended ACL.
link-group {**num**	**name** }	Specifies a Layer 2 ACL.
subitem *subitem*	Specifies the sub item in the ACL.

Command Modes Global Configuration (config)

Command Default None

Example

The following example shows how to copy packets that match the subitem number 2 of ACL numbered 3 to CPU:

```
Device#configure terminal
Device(config)#traffic-copy-to-cpu ip-group 3 subitem 2
```

traffic-redirect

To redirect the messages sent to a port, use the **traffic-redirect** command in the global configuration mode. To remove the redirect configuration, use the **no** form of the command.

[**no**] **traffic-redirect** { [**ip-group** {**num** | **name** } [**subitem** *subitem*]] [**link-group** {**num** | **name** } [**subitem** *subitem*]] [**interface** *interface-num* | **cpu**] }

ip-group {**num**	**name** }	Specifies a standard or extended ACL.
link-group {**num**	**name** }	Specifies a Layer 2 ACL.
subitem *subitem*	Specifies the sub item in the ACL.
interface *interface-num*	Specifies the interface to which the traffic is redirected.
cpu	Specifies that the traffic is redirected to the CPU.

Command Modes Global Configuration (config)

Command Default None

Usage Guidelines Use the **traffic-redirect** command to forward the traffic to an egress port or a CPU, using the specified access control list (ACL) sub items.

Example

The following example shows how to redirect traffic to the ethernet 1/1 interface:

```
Device#configure terminal
Device(config)#traffic-redirect link-group link1 interface ethernet 1/1
```

traffic-statistic

To configure a device to collect traffic statistics, use the **traffic-statistic** command in in global configuration mode. To remove the traffic statistic configuration, use the **no** form of the command.

[**no**] **traffic-statistic** { [**ip-group** {**num** | **name** } [**subitem** *subitem*]] [**link-group** {**num** | **name** } [**subitem** *subitem*]] }

ip-group {**num** | **name** }	Specifies a standard or extended ACL.
link-group {**num** | **name** }	Specifies a Layer 2 ACL.
subitem *subitem*	Specifies the sub item in the ACL.

Command Modes

Global Configuration (config)

Command Default

None

Usage Guidelines

Use this command to configure the device to collect traffic statistics. This command displays a cumulative value of the count of the number of packets that matched the ACL rule.

If you reconfigure traffic statistics, the previous information is lost.

Example

```
Device#configure terminal
Device(config)#traffic-statistic ip-group 3
```

PART VII

Security

Security

absolute time-range

To configure an absolute time range that specifies when an access control list (ACL) is in effect, use the **absolute** command in the time-range configuration mode. To remove the absolute time-range, use the **no** form of the command.

`[no]absolute [start` *time-range* `][end`*time-range* `]`

Syntax Description

time-range	Specifies the time in the format of HH:MM:SS YYYY/MM/DD

Command Modes

Global Configuration (config)

Command Default

None

Example

```
Device#configure terminal
Device(config)#time-range weekends
Device(config-timerange-weekends)#absolute start 04:50:30 2020/04/01 end 09:50:40 2020/04/30
```

access-limit

To enable or disable the number limit of authentication users in the domain and set the number limit of allowed users, use the **access-limit** commmand in AAA configuration mode.

access-limit {**enable** *allowed-user-number-limit* | **disable**}

Syntax Description

enable	Enables the number limit of authentic domain
allowed-user-number-limit	Sets the number limit of allowed user The range is from 1 to 640.
disable	Disables the number limit of authenti domain.

Command Modes

AAA configuration (config-aaa)

Example

This example shows how to enable the number limit of authentication users in the domain and set the number limit of allowed users:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# domain eee
Device(config-aaa-domain-eee)# exit
Device(config-aaa)# default domain-name enable eee
Device(config-aaa)# domain eee
Device(config-aaa-domain-eee)# access-limit enable 3
 Succeed to set MaxLinks of domain.
```

Example

This example shows how to disable the number limit of authentication users in the domain and set the number limit of allowed users:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# default domain-name enable eee
 Succeed in setting default domain.
Device(config-aaa)# domain eee
Device(config-aaa-domain-eee)# access-limit disable
 Succeed to disable access limit of domain.
```

access-list match-order

To configure the access control list (ACL) matching order, use the **access-list match-order** command in the global configuration mode. The matching order decides which rule is executed.

```
access-list acl-nummatch-order {auto |config}
```

Syntax Description

auto	Matches the ACL rules according to the depth-first rule, wherein the longest subitem in a rule takes priority. The longest subset of a rule is matched first before the rule.
config	Matches the ACL rules according to the configuration order.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

An ACL consists of multiple permit or deny rules. The rules may overlap or conflict. In such cases, the matching order decides which rule is executed.

Example

```
Device#configure terminal
Device(config)#access-list 2 match-order config
```

access-group

To activate an access control list that is already defined, use the **access-group** command in the global configuration mode.

access-group [**ip-group** [*name* | *number*]] [**link-group** [*name* | *number*]] [**subitem** *number*]

Syntax Description

ip-group [*name*	*number*]	Specifies a predefined Standard ACL or Extended ACL.
link-group [*name*	*number*]	Specifies a predefined Layer 2 ACL.
subitem *number*	Specifies the sub item number in the ACL

Command Modes

Global Configuration (config)

Command Default

None

Usage Guidelines

After defining an Access Control List (ACL), it has to be activated to take effect. Use the **access-group ip-group** command to activate a Standard ACL or an Extended ACL. Use the **access-group link-group** command to activate a Layer 2 ACL.

Example

The following example creates a standard access control list (ACL), 10, and activates the subitem number 1 of the ACL.

```
Device#configure terminal
Device(config)#access-list 10 deny any

Device(config)#access-list 10 permit 10.1.1.5 0
Device(config)#access-group ip-group 10
```

access-list numbered standard

To define a numbered Standard Access Control List (ACL), use the **access-list** *number* command in the global configuration mode.

```
access-list num{permit |deny} { source-ipv4 | ipv6-source-prefix | any | ipv6any}
[ time-range timerange-name]
```

Syntax Description

permit	Specifies that the rule defined by the ACL is permitted.
deny	Specifies that the rule defined by the ACL is not permitted.
source-ipv4	Specifies the IPv4 address of the source host.
ipv6-source-prefix	Specifies the IPv6 prefix of the source host.
ipv6any	Specifies any IPv6 host
any	Specifies any IPv4 host
time-range*timerange-name*	Defines the specific time range to implement the ACL.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

The ACL is identified by the number assigned to it. You can create an ACL and assign a number to it. If you don't specify a number, the system assigns a number to the created ACL. For a Standard ACL, the numbers range from 1 through 99. You can create upto 99 Standard ACLs.

Example

```
Device#configure terminal
Device(config)#access-list 10 permit any
```

access-list standard

To create a named Standard Access Control List, use the **access-list standard** command in the global configuration mode.

```
access-list standard {num|name }[ match-order { auto | config }]
```

Syntax Description

num	Specifies a standard ACL. Values can range from 1 through 99.
name	Specifies a name for the ACL. The name is a string of alphanumeric characters, upto 32 characters in length.
match-order	Defines a matching order for the entries in the ACL.
config	Matches the ACL rules according to the configuration order in the list.
auto	Matches the ACL rules according to the depth-first rule, wherein the longest subitem in a rule takes priority. The longest subset of a rule is matched first before the rule.

Command Default

None

Command Modes

Global configuration (config)

Example

```
Device#configure terminal
Device(config)#access-list standard stdacl
```

accounting-on

To configure accounting-on fucntion, use the **accounting-on** command in AAA configuration mode.

accounting-on {**enable** *packet-number* | **disable**}

Syntax Description

enable	Enables accounting-on function.
packet-number	The number of accounting-on pacl The range is 1 to 255.
disable	Disables accounting-on function.

Command Modes

AAA configuration (config-aaa)

Example

This example shows how to enable the accounting-on function:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# accounting-on enable 10
 configure success
```

acct-secret-key

To configure the shared key of the secondary RADIUS server, use the **acct-secret-key** command in AAA configuration mode. To delete the configured shared key of the secondary RADIUS server, use the **no** form of the command.

acct-secret-key*key*

no acct-secret-key

Syntax Description

key	The shared secret key.

Command Modes

AAA Configuration (config-aaa)

Example

This example shows how to configure the shared key of a secondary RADIUS server using the **acct-secret-key** command:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius host radius1
Device(config-aaa-radius-radius1)# acct-secret-key 1
 Modify secret key of RADIUS configuration successfully
```

anti-dos ip fragment

To configure a new threshold value for IP fragmentations, use the **anti-dos ip fragment** command in global configuration mode. To restore the default threshold value, use the **no** form of the command.

anti-dos ip fragment *threshold-value*

no anti-dos ip fragment

Syntax Description

threshold-value	The maximum number of allowed The range is 0 to 800. The default value is 800.

Command Modes

Global Configuration (config)

Example

This example shows how to configure a new threshold value for IP fragmentations using the **anti-dos ip fragment** command:

```
Device> enable
Device# configure terminal
Device(config)# anti-dos ip fragment 100
```

anti-dos ip ttl

To enable TTL monitoring and anti-TTL attack, use the **anti-dos ip ttl** command in global configuration mode. To disable TTL monitoring and anti-TTL attack, use the **no** form of the command.

anti-dos ip ttl

no anti-dos ip ttl

Command Default Messages with TTL with a value of 0 are discarded.

Command Modes Global Configuration (config)

Example

This example shows how to enable TTL monitoring using the **anti-dos ip ttl** command:

```
Device> enable
Device# configure terminal
Device(config)# anti-dos ip ttl
```

arp anti-spoofing

To enable ARP anti-spoofing, use the **arp anti-spoofing** command in global configuration mode. To disable ARP anti-spoofing, use the **no** form of the command.

arp anti-spoofing

no arp anti-spoofing

Command Modes

Global Configuration (config)

Example

This example shows how to enable ARP anti-spoofing using the **arp anti-spoofing** command:

```
Device> enable
Device# configure terminal
Device(config)# arp anti-spoofing
Device(config)#
```

arp anti-spoofing deny-disguiser

To enable ARP gateway anti-spoofing, use the **arp anti-spoofing deny-disguiser** command in global configuration mode. To disable ARP gateway anti-spoofing, use the **no** form of the command.

arp anti-spoofing deny-disguiser

no arp anti-spoofing deny-disguiser

Command Modes

Global Configuration (config)

Example

This example shows how to enable ARP gateway anti-spoofing using the **arp anti-spoofing deny-disguiser** command:

```
Device> enable
Device# configure terminal
Device(config)# arp anti-spoofing deny-disguiser
Device(config)#
```

arp anti-spoofing unknown

To enable ARP anti-spoofing and configure the device to flood or disable unknown packets, use the **arp anti-spoofing unknown** command in global configuration mode.

arp anti-spoofing unknown {**flood** | **disable**}

Syntax Description

flood	Floods the unknown packets.
disable	Disables the unknown packets.

Command Modes

Global Configuration (config)

Example

This example shows how to flood the unknown packets using the **arp anti-spoofing unknown flood** command:

```
Device> enable
Device# configure terminal
Device(config)# arp anti-spoofing unknown flood
Device(config)#
```

Example

This example shows how to disable the unknown packets using the **arp anti-spoofing unknown disable** command:

```
Device> enable
Device# configure terminal
Device(config)# arp anti-spoofing unknown disable
Device(config)#
```

arp anti-spoofing valid-check

To enable ARP anti-spoofing and configure source MAC address consistency inspection, use the **arp anti-spoofing valid-check** command in global configuration mode. To disable source MAC address consistency inspection, use the **no** form of the command.

arp anti-spoofing valid-check

no arp anti-spoofing valid-check

Command Modes

Global Configuration (config)

Example

This example shows how to enable source MAC address consistency inspection using the **arp anti-spoofing valid-check** command:

```
Device> enable
Device# configure terminal
Device(config)# arp anti-spoofing valid-check
Device(config)#
```

arp anti-flood

To enable ARP anti-flooding attack and configure its parameters on all ports, use the **arp anti-flood** command in global configuration mode.

To enable ARP anti-flooding attack and configure its parameters on a specific port, use the **arp anti-flood** command in interface configuration mode.

To disable ARP anti-flooding attack, use the **no** form of the command.

arp anti-flood [[**action** {**deny-all** | **deny-arp**}] [**threshold** *threshold-value*] | **recover** {*mac-address* | **all**} | **recover-time** *time*]

no arp anti-flood [**recover-time** | **threshold**]

Syntax Description

action deny-all	Adds the host to a blackhole addre packets.
action deny-arp	Adds the host to a blackhole addre ARP packets.
threshold *threshold-value*	Configures the ARP anti-flood thr The default value is 16 packets pe
recover *mac-address*	Manually restores the host with the to transmit again.
recover all	Manually restores all the hosts to t
recover-time *time*	Defines the recovery time interval allowed to transmit again. The recovery interval is 0 to 1440 The default value is 10 minutes.

Command Modes

Global configuration (config)
Interface configuration (config-if)

Example

This example shows how to configure ARP anti-flooding attack using the **arp anti-flood** command:

```
Device> enable
Device# configure terminal
Device(config)# arp anti-flood
Device(config)#
```

Example

This example shows how to add the host to a blackhole address list and discard all packets using the **arp anti-flood action deny-all** command:

```
Device> enable
Device# configure terminal
Device(config)# arp anti-flood action deny-all
Device(config)#
```

Example

This example shows how to configure ARP anti-flooding threshold value using the **arp anti-flood threshold** *threshold-value* command:

```
Device> enable
Device# configure terminal
Device(config)# arp anti-flood threshold 30
Device(config)#
```

Example

This example shows how to manually restore the host to transmit again using the **arp anti-flood recover** command:

```
Device> enable
Device# configure terminal
Device(config)# arp anti-flood recover 00:00:00:00:32:33
Device(config)#
```

Example

This example shows how to define the recovery time interval after which a host is allowed to transmit again using the **arp anti-flood recover-time** *time* command:

```
Device> enable
Device# configure terminal
Device(config)# arp anti-flood recover-time 100
Device(config)#
```

channel-group spanning-tree cost

To configure the path cost of an STP aggregation group, use the **channel-group** *group-id* **spanning-tree cost** command in global configuration mode. To restore the default path cost of an STP aggregation group, use the **no** form of the command.

channel-group *group-id* **spanning-tree cost** *path-cost*

no channel-group *group-id* **spanning-tree cost**

Syntax Description

group-id	The channel group ID. The range is 0 to 5.
path-cost	The path cost of the aggregation g The range is 1 to 200000000.

Command Modes

Global configuration (config)

Example

This example shows how to configure the path cost of an aggregation group using the **channel-group** *group-id* **spanning-tree cost** command:

```
Device> enable
Device# configure terminal
Device(config)# channel-group 1 spanning-tree cost 2000
Device(config)#
```

clear cpu-classification

To clear the CPU packet classification statistics, run the **clear cpu-classification** command in global configuration mode.

clear cpu-classification interface {**ethernet** | **gpon**}*slot-number/port-number*

Syntax Description

slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1 • 10GE Ethernet: The value is • *port-number*: • GPON: The range is from 1 • GE Ethernet: The range is f • 10GE Ethernet: The range is

Command Default

None

Command Modes

Global configuration (config)

Example

This example shows how to clear the CPU packet classification statistics:

```
Device> enable
Device# configure terminal
Device(config)# clear cpu-classification interface ethernet 1/3
Clear packets sent to cpu classification statistics successfully
```

clear cpu-statistics

To clear the port statistics, use the **clear cpu-statistics** command in privileged EXEC and global configuration modes.

clear cpu-statistics

Command Default

None

Command Modes

Privileged EXEC (#)
Global configuration (config)

Examples

This example shows how to clear the port statistics.

```
Device> enable
Device# configure terminal
Device(config)# clear cpu-statistics
Clear packet sent to cpu statistic information successfully
```

cpu-car

To configure the CPU-car rate limit for packets, use the **cpu-car** command in global configuration mode. To restore the default CPU-car rate limit, use the **no** form of the command.

cpu-car *rate-limit*

no cpu-car

Syntax Description

rate-limit	Configures the CPU-car rate limit. The range is 1 to 10000 packets per se The default value is 4000 packets per

Command Modes

Global configuration (config)

Example

This example shows how to configure real time accounting using the **realtime-account** command:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius host radius1
Device(config-aaa-radius-radius1)# realtime-account interval 25
 Modify realtime_acct configuration of radius server successfully.
```

cpu-limit

To configure the CPU limit rate for packet types, use the **cpu-limit** command in global configuration mode. To restore the default CPU limit rate for packet types, use the **no** form of the command.

cpu-limit { **arp** | **bpdu** | **broadcast** | **dhcp** | **icmp** | **igmp** | **mld** | **ospf** | **other** | **rip** | **snmp** | **ssh** | **switch-dst-mac** | **telnet** } *rate*

no cpu-limit

Syntax Description

rate	Configures the CPU-limit rate. The range is 1 to 10000 packets per second.

Command Default

By default, no limit is configured.

Command Modes

Global configuration (config)

Example

This example shows how to configure CPU limit rate for ARP packets:

```
Device> enable
Device# configure terminal
Device(config)# cpu-limit arp 100
```

dhcp anti-attack

To enable DHCP packet monitoring and configure the monitoring parameters on all ports, use the **dhcp anti-attack** command in global configuration mode.

To enable DHCP packet monitoring and configure the monitoring parameters on a specific port, use the **dhcp anti-attack** command in interface configuration mode.

To disable DHCP packet monitoring and restore the parameters to their default values, use the **no** form of the command.

dhcp anti-attack [[**action** {**deny-all** | **deny-dhcp**}] [**threshold** *threshold-value*] | [**bind blackhole** | **recover**] {*mac-address* | **all**} | **recover-time** *time*]

no dhcp anti-attack [**recover-time** | **threshold**]

Syntax Description

action deny-all	Adds the host to a blackhole address l packets.
action deny-dhcp	Adds the host to a blackhole address li DHCP packets.
threshold *threshold-value*	Configures the rate threshold for DHC The default value is 16 packets per se
bind blackhole *mac-address*	Binds the dynamic MAC address gene the static MAC address for the specifi the blackhole address list.
bind blackhole all	Binds the dynamic MAC address gene the static MAC address for all the MA blackhole address list.
recover *mac-address*	Manually restores the table items for t specified MAC address.
recover all	Manually restores the table items for a
recover-time *time*	Defines the recovery time interval. The recovery interval is 0 to 1440 mi The default value is 10 minutes.

Command Modes

Global configuration (config)
Interface configuration (config-if)

Example

This example shows how to configure DHCP packet monitoring using the **dhcp anti-attack** command:

```
Device> enable
Device# configure terminal
Device(config)# dhcp anti-attack
Device(config)#
```

Example

This example shows how to configure DHCP packet monitoring and discard all packets using the **dhcp anti-attack action deny-all** command:

```
Device> enable
Device# configure terminal
Device(config)# dhcp anti-attack action deny-all
Device(config)#
```

Example

This example shows how to configure the threshold value for DHCP packet globally using the **dhcp anti-attack threshold** command:

```
Device> enable
Device# configure terminal
Device(config)# dhcp anti-attack threshold 10
Device(config)#
```

Example

This example shows how to manually restore the table items for the host using the **dhcp anti-attack recover** command:

```
Device> enable
Device# configure terminal
Device(config)# dhcp anti-attack recover all
Device(config)#
```

Example

This example shows how to configure recovery time interval using the **dhcp anti-attack recover-time** command:

```
Device> enable
Device# configure terminal
Device(config)# dhcp anti-attack recover-time 100
Device(config)#
```

discard-bpdu

To enable the local discard of external BPDU messages, use the **discard-bpdu** command in global configuration mode. To disable the local discard of external BPDU messages, use the **no** form of the command.

discard-bpdu

no discard-bpdu

Command Modes

Global configuration (config)

Example

This example shows how to enable the local discard of external BPDU messages using the **discard-bpdu** command:

```
Device> enable
Device# configure terminal
Device(config)# discard-bpdu
Enable discard bpdu successfully.
```

access-list extended name

To create a named Extended Access Control List, use the **access-list extended** command in the global configuration mode.

```
access-list extended {num|name }[ match-order { auto | config }]
```

Syntax Description

num	Specifies an extended ACL. Values can range from 100 through 199.
name	Specifies a name for the ACL. The name is a string of alphanumeric characters, upto 32 characters in length.
match-order	Defines a matching order for the entries in the ACL.
config	Matches the ACL rules according to the configuration order in the list.
auto	Matches the ACL rules according to the depth-first rule, wherein the longest subitem in a rule takes priority. The longest subset of a rule is matched first before the rule.

Command Default

None

Command Modes

Global configuration (config)

Example

```
Device#configure terminal
Device(config)#access-list extended extacl match-order auto
```

access-list numbered extended

To define a numbered Extended Access Control List (ACL), use the **access-list** *number* command in the global configuration mode.

`access-list` *number* `{permit |deny} [protocol ] [established] {` *source-ipv4* `|` *ipv6-source-prefix* `| any | ipv6any}[`*source-port-wildcard*`]{` *dest-ipv4* `|` *ipv6-dest-prefix* `| any | ipv6any}[`*dest-port-wildcard*`][` *icmp type icmp-code*`][`*igmp-type*`] [ traffic-class` *traffic-class* `][ precedence` *precedence* `][ tos` *tos* `][ dscp` *dscp*`][ fragments ][ time-range` *time-range* `]`

Syntax Description

permit	Specifies that the rule defined by the ACL is permitted.
deny	Specifies that the rule defined by the ACL is not permitted.
protocol	Specifies the type of Layer 2 protocol. It is in the range of 1 through 255 by number. Select from GRE, ICMP, IGMP, IPinIP, OSPF, TCP, UDP, and ICMPv6 to specify the protocol by name.
established	Defines the SYN flag in TCP. A value 1 indicates that the flag is active. This is applicable only if the *protocol* is tcp.
source-ipv4	Specifies the IPv4 address of the source host.
ipv6-source-prefix	Specifies the IPv6 prefix of the source host.
ipv6any	Specifies any IPv6 host
dest-ipv4	Specifies the IPv4 address of the destination host.
ipv6-dest-prefix	Specifies the IPv6 prefix of the destination host.
any	Specifies any host.
icmp type icmp-code	Specifies the type of ICMP protocol packet. It is valid only when protocol is configured as **icmp** or **icmpv6**.
igmp-type	Specifies the type of IGMP protocol packet. It is valid only when protocol is configured as **igmp**.
traffic-class	Specifies the traffic class for IPv6.
precedence	Specifies the precedence priority. IP precedence ranges from 0 through 7.
tos	Specifies the Type of Service (ToS) priority. The values range from 0 through 15.
dscp	Specifies the Differentiated Services Code Point (DSCP) priority value.
fragments	Specifies that the ACL rule is valid for non-first fragmented packets. This helps prevent fragment packet attacks.

time-range*timerange-name*	Defines the specific time range to implement the ACL.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

The ACL is identified by the number assigned to it. You can create an ACL and assign a number to it. If you don't specify a number, the system assigns a number to the created ACL. For an Extended ACL, the numbers range from 100 through 199. You can create upto 100 Extended ACLs.

Example

```
Device#configure terminal
Device(config)#access-list 101 permit tcp 10.0.0.1 0 ftp any
```

host-guard bind ip

To configure host protection on a port, use the **host-guard bind ip** command in global configuration mode. To disable host protection on a port, use the **no** form of the command.

host-guard bind ip *ip-address* **interface** { **ethernet** *slot_number/port_number* | **gpon** *slot_number/port_number* } [**to** | **ethernet** *slot_number/port_number* | **gpon** *slot_number/port_number*]

no host-guard bind ip *ip-address* **interface** { **ethernet** *slot_number/port_number* | **gpon** *slot_number/port_number* } [**to** | **ethernet** *slot_number/port_number* | **gpon** *slot_number/port_number*]

Syntax Description

to	Displays the information for a range o the **to** keyword, specify the same port t the keyword.
slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1 • 10GE Ethernet: The value is • *port-number*: • GPON: The range is from 1 • GE Ethernet: The range is fi • 10GE Ethernet: The range is

Command Modes

Global configuration (config)

Examples

This example shows how to configure host protection on a port using the **host-guard bind ip** command:

```
Device> enable
Device# configure terminal
Device(config)# host-guard bind ip 10.10.10.1 interface ethernet 1/3
 Add host guard entry successfully.
```

ip route

To add a static IP route to the routing table, use the **ip route** command in the global configuration mode. To remove a static IP route from the routing table, use the **no** form of the command.

ip route *dest-ip mask* [*gate-ip*]

no ip route *dest-ip mask* [*gate-ip*]

Syntax Description

dest-ip	The destination address of the stati added.
mask	The mask of the destination addres
gate-ip	The next-hop address of the static

Command Modes

Global configuration (config)

Example

This example shows how to add a static IP route to the routing table using the **ip route** command:

```
Device> enable
Device# configure terminal
Device(config)# ip route 10.10.10.10 255.255.0.0 10.0.11.254
```

access-list link name

To create a named Layer 2 Access Control List (ACL), use the **access-list link** command in the global configuration mode.

```
access-list link {num|name }[ match-order { auto | config }]
```

Syntax Description

num	Specifies an extended ACL. Values can range from 200 through 299.
name	Specifies a name for the ACL. The name is a string of alphanumeric characters, upto 32 characters in length.
match-order	Defines a matching order for the entries in the ACL.
config	Matches the ACL rules according to the configuration order in the list.
auto	Matches the ACL rules according to the depth-first rule, wherein the longest subitem in a rule takes priority. The longest subset of a rule is matched first before the rule.

Command Default

None

Command Modes

Global configuration (config)

Example

```
Device#configure terminal
Device(config)#access-list link laye2acl match-order auto
```

access-list link number

To define a numbered Layer 2 Access Control List (ACL), use the **access-list** *number* command in the global configuration mode.

`access-list` *number* `{permit |deny} [protocol ] [cos` *vlan-priority*`] ingress { { [inner-vid`*vid* `][`*start-vlan-id end-vlan-id* `] [`*source-mac-addr source-mac-wildcard*`][interface` *interface-number* `]} |any } egress { { [`*dest-mac-addr dest-mac-wildcard* `][interface` *interface-num* `| cpu]} | any}[ time-range` *time-range* `]`

Syntax Description

permit	Specifies that the rule defined by the ACL is permitted.
deny	Specifies that the rule defined by the ACL is not permitted.
protocol	Specifies the type of protocol packet carried by the Ethernet frame. In hexadecimal notation, the range is 0 through FFFF. It is optional in case of ARP, IP, RARP.
cos	Defines the SYN flag in TCP. A value 1 indicates that the flag is active. This is applicable only if the *protocol* is tcp.
ingress	Specifies the rule for the incoming packets at the ingress port.
inner-vid	Specifies the inner VLAN ID of a double-tagged packet.
start-vlan-id end-vlan-id	Specifies the range of VLANs. For a double-tagged packet, it is the VLAN ID of the outer tag.
source-mac-addr source-mac-wildcard	Specifies the source MAC address options. *source-mac-wildcard* indicates the source MAC range.
interface *interface-num*	Specifies the physical port number. It can be either the ingress port or the egress port.
CPU	Indicates that the data will be forwarded to the CPU.
any	Specifies any address which can be at ingress or egress directions.
time-range *name*	Specifies the time range in which the ACL rule takes effect.
time-range*timerange-name*	Defines the specific time range to implement the ACL.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

The ACL is identified by the number assigned to it. You can create an ACL and assign a number to it. If you don't specify a number, the system assigns a number to the created ACL. For an Extended ACL, the numbers range from 200 through 299. You can create upto 100 Layer 2 ACLs.

Example

```
Device# configure terminal
Device(config)# access-list 201 permit arp ingress 00:00:00:00:01:01 0 egress any
```

local-user

To configure a local user, use the **local-user** command in the AAA configuration mode. To delete all local users, use the **no** form of the command.

local-user username *username* **password** *password* [**vlan** *vlan-id*]

no local-user {**all** | **user** *username*}

Syntax Description

username	Username of the local user.
password	Password of the local user.
vlan-id	The VLAN ID. The range is 1 to 4094.

Command Modes

AAA configuration (config-aaa)

Example

This example shows how to configure a local user using the **local-user** command:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# local-user username name1 password pass1 vlan 220
Device(config-aaa)#
```

nas-ipaddress

To configure the NAS client IP address for a RADIUS server, use the **nas-ipaddress** command in AAA configuration mode. To delete the configured NAS client IP address for a RADIUS server, use the **no** form of the command.

nas-ipaddress *ip-address*

no nas-ipaddress

Syntax Description

ip-address	IP address of RADIUS client.

Command Modes

AAA configuration (config-aaa)

Example

This example shows how to configure the NAS client IP address for a RADIUS server:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius host radius1
Device(config-aaa-radius-radius1)# nas 10.1.1.10
```

no ip route static all

To delete all static IP routes from the routing table, use the **no ip route static all** command in global configuration mode.

no ip route static all

Command Modes

Global configuration (config)

Example

This example shows how to delete all static IP routes from the routing table using the **no ip route static all** command:

```
Device> enable
Device# configure terminal
Device(config)# no ip route static all
```

periodic time-range

To configure a time period that specifies when an access control list (ACL) is in effect, use the **periodic** command in the time-range configuration mode. To remove the absolute time-range, use the **no** form of the command.

`[no]periodic [`*days-of-week*`] HH:MM:SS to [`*days-of-week* `] HH:MM:SS`

Syntax Description

days-of-week	Specifies the period, which are the days of the week: **mon**, **tue**, **wed**, **thu**, **fri**, **sat**, **sun**, **weekdays**, daily **weekdays** are Monday to Friday.
HH:MM:SS	Specifies the time in *hours*:*minutes*:*seconds* format.

Command Modes

Global Configuration (config)

Command Default

None

Example

```
Device#configure terminal
Device(config)#time-range days
Device(config-timerange-days)#periodic daily 04:50:30 to 09:50:40
```

preemption-time

To configure the recovery time to switch to the primary server, use the **preemption-time** command in AAA configuration mode.

preemption-time *time*

Syntax Description

time	The preemption time The unit in minutes. The range is from 0 to 1440. The default value isc0

Command Modes

AAA configuration (config-aaa)

Usage Guidelines

Use this command in the AAA configuration mode.

Examples

This example shows how to configure the recovery time to switch to the primary server.

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius host radius1
Device(config-aaa-radius-radius1)# preemption-time 200
```

Related Commands

Command	Description
aaa	Enters AAA configuration mode

{primary-acct-ip | second-acct-ip}

To configure the primary and secondary accounting servers, use the {**primary-acct-ip** |**second-acct-ip**} *ip_address port* command in AAA configuration mode. To disable the configured primary and secondary accounting servers, use the **no** form of the command.

{**primary-acct-ip** | **second-acct-ip**}*ip_address port*

no {**primary-acct-ip** | **second-acct-ip**}

Syntax Description

primary-acct-ip	The primary accounting server.
second-acct-ip	The secondary accounting server.
ip_address	The IP address of the server.
port	The accounting port The range is from 1 to 65535.

Command Modes

AAA configuration (config-aaa)

Examples

This example shows how to configure the primary and secondary accounting server.

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius host radius1
Device(config-aaa-radius-radius1)# primary-acct-ip 10.1.1.10 333
Device(config-aaa-radius-radius1)# second-acct-ip 10.1.1.11 350
```

{primary-auth-ip | second-auth-ip}

To configure the primary and secondary RADIUS servers, use the {**primary-auth-ip** |**second-auth-ip**} *ip_address port* command in AAA configuration mode. To disable the configured primary and secondary RADIUS servers, use the **no** form of the command.

{**primary-auth-ip** | **second-auth-ip**} *ip_address port*

no {**primary-auth-ip** | **second-auth-ip**}

Syntax Description

primary-auth-ip	The primary RADIUS server.
second-auth-ip	The secondary RADIUS server.
ip_address	The IP address of the server.
port	The server port The range is from 1 to 65535.

Command Default

None

Command Modes

AAA configuration (config-aaa)

Examples

This example shows how to configure the primary and secondary accounting server

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius host radius1
Device(config-aaa-radius-radius1)# primary-auth-ip 10.2.1.10 80
Device(config-aaa-radius-radius1)# second-auth-ip 10.2.1.11 90
```

radius

To configure the RADIUS server parameters, use the **radius** command in AAA configuration mode. To restore the default RADIUS server settings, use the **no** version of the command.

radius {**8021p enable** | **accounting** | **attribute client-version** | **bandwidth-limit enable** | **config-attribute** {**access-bandwidth** {**downlink** *vendor-type* | **unit** {**bps** | **kbps**} | **uplink***vendor-type*} | **dscp** *vendor-type* | **mac-address-number** *vendor-type*} | **host** *host-name* | **mac-address-number enable** | **server-disconnect drop1x** | **vlan enable**}

no radius {**8021p** | **accounting** | **attribute client-version** | **bandwidth-limit enable** | **host** *host-name* | **mac-address-number** | **server-disconnect drop1x** | **vlan**}

Syntax Description

8021p enable	Configures RADIUS to distribute por
accounting	Enables accounting function.
attribute client-version	Send the H3C client's version to radiu
bandwidth limit-enable	Configures RADIUS to distribute ban
config-attribute	Configures the RADIUS attribute typ attributes.
access-bandwidth	Configures the RADIUS access bandv
downlink	Configures the RADIUS downlink att
uplink	Configures the RADIUS uplink attrib
unit bps	Configures the RADIUS ACL bandw per second.
unit kbps	Configures the RADIUS ACL bandw kilobits per second.
dscp	Configures the RADIUS DSCP attribu
config-attribute mac-address-number	Configures the maximum MAC addre learned for the RADIUS server.
vendor-type	The vendor type. The range is from 1 to 500.
mac-address-number enable	Configures RADIUS to distribute nun address.
host *host-name*	Creates a RADIUS scheme and enters mode for the specified host name.
server-disconnect drop1x	Configures the device to shut the user accounting packet does not respond.

vlan enable	Configures RADIUS to distribute

Command Modes AAA configuration (config-aaa)

Example

This example shows how to configure RADIUS to distribute port priority:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius 8021p enable
 Configure successfully.
```

Example

This example shows how to enable accounting function:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius accounting
 Modify accounting configuration of radius server successfully.
```

Example

This example shows how to send the H3C client's version to radius server:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius attribute client-version
Device(config-aaa)#
```

Example

This example shows how to configure RADIUS to distribute bandwidth control:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius bandwidth limit-enable
 Configure successfully.
```

Example

This example shows how to configure the RADIUS access bandwidth and downlink attribute:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius config-attribute access-bandwidth downlink 400
 Configure successfully.
```

Example

This example shows how to configure the RADIUS DSCP attribute:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius config-attribute dscp 1
 Configure successfully.
```

Example

This example shows how to create a RADIUS scheme and enters RADIUS scheme mode:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius host hostname1
Device(config-aaa-radius-hostname1)#
```

Example

This example shows how to configure RADIUS to distribute number limit of MAC address:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius mac-address-number enable
 Configure successfully.
```

Example

This example shows how to shut the user down if the accounting packet does not respond:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius server-disconnect drop 1x
 Configure successfully.
```

Example

This example shows how to configure RADIUS to distribute port PVID:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius vlan enable
 Configure successfully.
```

realtime-account

To configure realtime accounting and its time interval, use the **realtime-account** command in AAA configuration mode. To disable realtime accounting, use the **no** form of the command.

realtime-accountinterval*time*

no realtime-account

Syntax Description

interval *time*	Configures the realtime accountin The range is 1 to 255 minutes.

Command Modes

AAA configuration (config-aaa)

Example

This example shows how to configure real time accounting using the **realtime-account** command:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius host radius1
Device(config-aaa-radius-radius1)# realtime-account interval 25
 Modify realtime_acct configuration of radius server successfully.
```

no access-list

To remove an entry or all entries from the Access Control List (ACL), use the **no access-list** command in the global configuration mode.

```
no access-list {number| name |all}
```

Syntax Description

number	Specifies that numbered ACL to delete
name	Specifies the name of the ACL to delete.

Command Default

None

Command Modes

Global configuration (config)

Example

```
Device#configure terminal
Device(config)#no access-list 10
```

scheme

To configure the server authentication scheme, use the **scheme** command in AAA configuration mode.

scheme {**local** | **radius** [**local**] }

Syntax Description

local	Configures to use local user authe
radius	Configures to use RADIUS server
radius local	Configures to use local user authe server authentication fails.

Command Modes

AAA configuration (config-aaa)

Example

This example shows how to configure a server authentication scheme using the **scheme** command:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# domain eee
Device(config-aaa-domain-eee)# scheme radius
Device(config-aaa-domain-eee)#
```

show access-list config

To display the Access Controlled List (ACL) configurations, use the **show access-list config** command in the EXEC mode

show access-list config {*number* | **all** | **name** | **statistic** }

Syntax Description

number	Specifies the numbered ACL. Numbers 1 to 99 represent standard ACL Numbers 100 to 199 represent extended A Numbers 200 to 299 represent Layer 2 A
all	Specifies all ACLs.
name	Specifies an ACL by name.
statistic	Specifies ACL statistics.

Command Modes

EXEC

Command Default

None

Usage Guidelines

Use the **show access-list config statistic** command to see the statistics of the ACL rules usage.

Use the **show access-list config name** command to see the ACL specified by name.

Use the **show access-list config all** command to all see the ACLs.

Examples

```
Device> enable
Device# show access-list config 1
Standard IP Access List 1, match-order is config, 2 rule:
  0  deny    any
permit  1.1.1.1  0.0.0.0
```

show access-list runtime

To display the Access Controlled List (ACL) at run time, use the **show access-list runtime** command in the EXEC mode

show access-list runtime {*number* | **all** | **name** | **statistic** }

Syntax Description

number	Specifies the numbered ACL. Numbers 1 to 99 represent standard A Numbers 100 to 199 represent extend Numbers 200 to 299 represent Layer
all	Specifies all ACLs.
name	Specifies an ACL by name.
statistic	Specifies ACL statistics.

Command Modes

EXEC

Command Default

None

Usage Guidelines

Use the **show access-list runtime statistic** command to see the statistics of the ACL rules usage.

Use the **show access-list runtime name** command to see the ACL specified by name.

Use the **show access-list runtime all** command to all see the ACLs.

Examples

```
Device> enable
Device# show access-list runtime 1
Standard IP Access List 1, match-order is config, 1 rule:
  0  deny    any
```

show anti-dos

To display the anti-DDOS configuration information, use the **show anti-dos** command in privileged EXEC or global configuration modes.

show anti-dos

Command Modes

Privileged EXEC (#)
Global Configuration (config)

Example

This example shows a sample output for the **show anti-dos** command:

```
Device> enable
Device# configure terminal
Device(config)# show anti-dos
Informations of AntiDos:
Ip fragment max number:800
Ip fragment number now:0
TTL=0 packet traffic to CPU is disable.
```

show arp anti-flood

To display the ARP anti-flood configuration and attackers list, use the **show arp anti-flood** command in privileged EXEC or global configuration modes.

show arp anti-floodport-threshold [{**ethernet** | **gpon**} *slot-number/port-number* [**to** {**ethernet** | **gpon**} *slot-number/port-number*]]

Syntax Description

slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value • 10GE Ethernet: The valu • *port-number*: • GPON: The range is fro • GE Ethernet: The range • 10GE Ethernet: The rang
to	Displays the information for a rang the **to** keyword, specify the same p the keyword.

Command Modes

Privileged EXEC (#)
Global Configuration (config)

Example

This example shows a sample output for the **show arp anti-flood** command:

```
Device> enable
Device# configure terminal
Device(config)# show arp anti-flood
Arp anti-flood: disabled
Arp rate limit:25pps
User recovery time:234 minutes
Reject type:DenyAll
DeniedSrcMAC       SourceIP         Port     Vlan  DenyType  RemainAgingTime(m)

Total entry:0.
```

Example

This example shows a sample output for the **show arp anti-flood port-threshold** command:

```
Device> enable
Device# configure terminal
Device(config)# show arp anti-flood port-threshold
Arp anti-flood: disabled
Arp rate limit:25pps
User recovery time:234 minutes
Reject type:DenyAll
Port        Port-threshold
g0/1        16
g0/2        16
g0/3        16
g0/4        16
g0/5        16
g0/6        16
g0/7        16
g0/8        16
e1/1        16
e1/2        16
e1/3        16
e1/4        16
e2/1        16
e2/2        16
```

show arp anti interface

To display the state of the interface, use the **show arp anti interface** command in privileged EXEC or global configuration modes.

show arp anti interface [{**ethernet** | **gpon**} *slot-number/port-number*]

Syntax Description

slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value • 10GE Ethernet: The valu • *port-number*: • GPON: The range is fro • GE Ethernet: The range • 10GE Ethernet: The rang

Command Modes

Privileged EXEC (#)
Global Configuration (config)

Example

This example shows a sample output for the **show arp anti interface** command:

```
Device> enable
Device# configure terminal
Device(config)# show arp anti interface
Port          mode          threshold(anti-flood)
g0/1          untrust       -
g0/2          untrust       -
g0/3          untrust       -
g0/4          untrust       -
g0/5          untrust       -
g0/6          untrust       -
g0/7          untrust       -
g0/8          untrust       -
e1/1          untrust       -
e1/2          untrust       -
e1/3          untrust       -
e1/4          untrust       -
e2/1          untrust       -
e2/2          untrust       -
```

show cpu-car

To display the CPU-car performance, use the **show cpu-car** command in privileged EXEC or global configuration modes.

show cpu-car

Command Modes

Privileged EXEC (#)
Global Configuration (config)

Example

This example shows a sample output for the **show cpu-car** command:

```
Device> enable
Device# configure terminal
Device(config)# show cpu-car
Send packet to cpu rate = 4000 pps.
```

show cpu-classification

To display CPU receiving packet classification statistics, run the **show cpu-classification** command in privileged EXEC or global configuration modes.

show cpu-classification [**interface** {**ethernet** | **gpon**}*slot-number/port-number*]

Syntax Description

slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1 • 10GE Ethernet: The value i • *port-number*: • GPON: The range is from 1 • GE Ethernet: The range is f • 10GE Ethernet: The range i

Command Default

None

Command Modes

Privileged EXEC(#)
Global Configuration(config)

Examples

This example shows how to view CPU receiving packet classification statistics.

```
Device> enable
Device# configure terminal
Device(config)# show cpu-classification
Type         Count       Percent(%)
Total        460699064   100

BPDU         8237424     1

ARP          378164060   82

IGMP         607189      0
ICMP         699125      0
OSPF         0           0
RIP          139         0
DHCP         12658100    2

SNMP         4079818     0

Telnet       122166      0
SSH          10788       0
Other        56120236    12
```

show cpu-limit

To display the packet types and the speed of each packet type, use the **show cpu-limit** command in privileged EXEC or global configuration modes.

show cpu-limit

Command Modes

Privileged EXEC (#)
Global Configuration (config)

Example

This example shows a sample output for the **show cpu-limit** command:

```
Device> enable
Device# configure terminal
Device(config)# show cpu-limit
packet-type     speed(pps)
other           200
broadcast       200
switch-dst-mac  1000
icmp            200
mld             200
igmp            200
ssh             200
dhcp            200
snmp            100
arp             100
ospf            200
rip             200
telnet          100
bpdu            200
```

show cpu-statistics

To display CPU receiving packet port statistics, use the **show cpu-statistics** command in privileged EXEC and global configuration modes.

show cpu-statistics [**channel-group** *channel-group-number* | {**gpon** | **ethernet**}*slot-number/port-number*] [**to** {**channel-group** *channel-group-number* | {**gpon** | **ethernet** }*slot-number/port-number*}]

Syntax Description

channel-group*channel-group-number*	The LACP channel group.
slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1 • 10GE Ethernet: The value i • *port-number*: • GPON: The range is from 1 • GE Ethernet: The range is f • 10GE Ethernet: The range i
to	Displays the information for a range o the same port type before and after th

Command Default

None

Command Modes

Privileged EXEC (#)
Global configuration (config)

Examples

This example shows how to view CPU receiving packet port statistics.

```
Device> enable
Device# configure terminal
Device(config)# show cpu-statistics ethernet 1/1
Show packets sent to cpu  statistic information
port  64Byte  128Byte  256Byte  512Byte  1024Byte  2048Byte
e1/1  0       0        0        0        0         0
```

show cpu-utilization

To display CPU utilization, use the **show cpu-utilization** command in global configuration mode.

show cpu-utilization

Command Default

None

Command Modes

Global configuration (config)

Examples

This example shows how to view CPU utilization.

```
Device> enable
Device# configure terminal
Device(config)# show cpu-utilization
CPU Information:
CPU Idle : 79 %
```

show dhcp anti-attack

To display the DHCP anti-attack configuration, use the **show dhcp anti-attack** command in privileged EXEC and global configuration modes.

show dhcp anti-attack [**interface** {**ethernet** | **gpon**} *slot-number/port-number* [**to** {**ethernet** | **gpon**} *slot-number/port-number*]]

Syntax Description

to	Displays the information for a rang the **to** keyword, specify the same po the keyword.
slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value • 10GE Ethernet: The valu • *port-number*: • GPON: The range is fro • GE Ethernet: The range • 10GE Ethernet: The rang

Command Modes

Privileged EXEC (#)
Global Configuration (config)

Example

This example shows a sample output for the **show dhcp anti-attack** command:

```
Device> enable
Device# configure terminal
Device(config)# show dhcp anti-attack
Dhcp anti-attack: enabled
Dhcp rate limit:1pps
User recovery time:3 minutes
Reject type:DenyDHCP
DeniedSrcMAC Port Vlan DenyType RemainAgingTime(m)
00:00:00:01:11:23 e1/1 2 DenyDHCP 3
Total entry: 1.
#After 3 minutes, the attack entry is aged out
```

show discard-bpdu

To display the BPDU status, use the **show discard-bpdu** command in privileged EXEC and global configuration modes.

show discard-bpdu

Command Modes

Privileged EXEC (#)
Global Configuration (config)

Example

This example shows a sample output for the **show discard-bpdu** command:

```
Device> enable
Device# configure terminal
Device(config)# show discard-bpdu
Discard BPDU global status: disable
Discard BPDU enable port:

Notes: Once global status is on, the switch will discard all BPDUs.
If want to enable on some ports only, need to disable global function and choose another
commands.
```

show dot1x

To display the 802.1x authentication function details, run the **show dot1x** command in privileged EXEC and global configuration modes.

show dot1x [[**daemon** | **detect** | **eapol-relay** | **guest-vlan**] [**interface** {**ethernet** | **gpon**} *slot-number/port-number*] [**to** {**ethernet** | **gpon**} *slot-number/port-number*] | **max-reauth** | **max-req** | **port-auth** | **quiet-period-value** | **session** [**interface** {**ethernet** | **gpon**} *slot-number/port-number* [**to** {**ethernet** | **gpon**} *slot-number/port-number*] | **mac-address** *mac-address-value*]]

Syntax Description

daemon	Displays the configuration of 802. interface watch function.
detect	Displays heartbeat detection confi
eapol-relay	Displays EAPOL pass through co
guest-vlan	Displays guest VLAN information
interface	Displays interface configuration, s control mode, re-authentication stat of users for the interface authentic
slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value • 10GE Ethernet: The valu • *port-number*: • GPON: The range is fro • GE Ethernet: The range • 10GE Ethernet: The rang
to	Displays the information for a ran the **to** keyword, specify the same p the keyword.
max-reauth	Displays information about maxim requests and identity packets sent
max-req	Displays information about the max requests sent by the server.

port-auth	Displays whether the interface authen or disabled.
quiet-period-value	Displays the quiet period.
session	Displays 802.1x session.
mac-address *mac-address-value*	Displays 802.1x session information fo address.

Command Modes

Privileged EXEC (#)
Global Configuration (config)

Example

This example shows the sample output for the **show dot1x daemon**

```
Device> enable
Device# configure terminal
Device(config)# show dot1x daemon
port  daemonstatus  daemontime(s)
g0/1  close         60
g0/2  close         60
g0/3  close         60
g0/4  close         60
g0/5  close         60
g0/6  close         60
g0/7  close         60
g0/8  close         60
e1/1  close         60
e1/2  close         60
e1/3  close         60
e1/4  close         60
e2/1  close         60
e2/2  close         60
```

Example

This example shows the sample output for the **show dot1x detect**

```
Device> enable
Device# configure terminal
Device(config)# show dot1x detect
the user detect interval is 25
port : detect
g0/1 : disable
g0/2 : disable
g0/3 : disable
g0/4 : disable
g0/5 : disable
g0/6 : disable
g0/7 : disable
g0/8 : disable
e1/1 : disable
e1/2 : disable
e1/3 : disable
e1/4 : disable
e2/1 : disable
```

```
e2/2 : disable

Total [14] item(s), printed [14] item(s).
```

Example

This example shows the sample output for the **show dot1x eapol-relay**

```
Device> enable
Device# configure terminal
Device(config)# show dot1x eapol-relay
Port  EapolRelay  EapolRelayUplink
g0/1  disabled    false
g0/2  disabled    false
g0/3  disabled    false
g0/4  disabled    false
g0/5  disabled    false
g0/6  disabled    false
g0/7  disabled    false
g0/8  disabled    false
e1/1  disabled    false
e1/2  disabled    false
e1/3  disabled    false
e1/4  disabled    false
e2/1  disabled    false
e2/2  disabled    false

Total entries: 14.
```

Example

This example shows the sample output for the **show dot1x guest-vlan**

```
Device> enable
Device# configure terminal
Device(config)# show dot1x guest-vlan
Port  GuestVlan  Status
g0/1  disable    InConfigVlan
g0/2  disable    InConfigVlan
g0/3  disable    InConfigVlan
g0/4  disable    InConfigVlan
g0/5  disable    InConfigVlan
g0/6  disable    InConfigVlan
g0/7  disable    InConfigVlan
g0/8  disable    InConfigVlan
e1/1  44         InConfigVlan
e1/2  disable    InConfigVlan
e1/3  disable    InConfigVlan
e1/4  disable    InConfigVlan
e2/1  disable    InConfigVlan
e2/2  disable    InConfigVlan

Total entries: 14.
```

Example

This example shows the sample output for the **show dot1x interface**

```
Device> enable
Device# configure terminal
Device(config)# show dot1x interface ethernet 1/3
Authentication of system: disabled
Type of authentication: eap-finish

Total [0] item(s).
```

Example

This example shows the sample output for the **show dot1x max-reauth**

```
Device> enable
Device# configure terminal
Device(config)# show dot1x max-reauth
the max-reauth is 2.
```

Example

This example shows the sample output for the **show dot1x max-req**

```
Device> enable
Device# configure terminal
Device(config)# show dot1x max-req
the max-req is 2.
```

Example

This example shows the sample output for the **show dot1x port-auth**

```
Device> enable
Device# configure terminal
Device(config)# show dot1x port-auth
--------------------------------------------------------------------------
port 1 auth is close
port 2 auth is close
port 3 auth is close
port 4 auth is close
port 5 auth is close
port 6 auth is close
port 7 auth is close
port 8 auth is close
port 9 auth is close
port 10 auth is close
port 11 auth is close
port 12 auth is close
port 13 auth is close
port 14 auth is close
--------------------------------------------------------------------------
```

Example

This example shows the sample output for the **show dot1x quiet-period-value**

```
Device> enable
Device# configure terminal
```

```
Device(config)# show dot1x quiet-period-value
the quiet-period-value is 0.
```

Example

This example shows the sample output for the **show dot1x session**

```
Device> enable
Device# configure terminal
Device(config)# show dot1x session
Total [0] item(s).
```

show ip route

To display the related information of specified routes as well as static routes, use the **show ip route** command in privileged EXEC and global configuration modes.

show ip route [*ip-address* [*mask*] | **ospf** | **rip** | **static**]

Syntax Description

ip-address	The destination address.
mask	The destination network segment prese
ospf	Displays all OSPF routes.
rip	Displays all RIP routes.
static	Displays all static routes.

Command Modes

Privileged EXEC (#)
Global Configuration (config)

Example

This example shows a sample output for the **show ip route** command:

```
Device> enable
Device# configure terminal
Device(config)# show ip route
Show ip route information

INET route table - vr: 0, table: 254
Route flag: U - up, G - gateway, H - host, R - reject, C - clone, S - static
Destination         Gateway             Flags    Use   Interface       Proto
0.0.0.0/0           10.75.171.1         UGS      659   VLAN-IF100      static
10.75.171.0/24      10.75.171.17        UC       5     VLAN-IF100      local
10.75.171.17        10.75.171.17        UH       0     lo0             local
127.0.0.0/8         127.0.0.1           UR       0     lo0             local
127.0.0.1           127.0.0.1           UH       4     lo0             local
192.168.100.0/24    192.168.100.1       UC       0     METH-IF0        local
192.168.100.1       192.168.100.1       UH       0     lo0             local

Total entries: 7. Printed entries: 7.
```

show radius

To display the RADIUS server details, run the **show radius** command in privileged EXEC mode.

show radius {**attribute** | **config-attribute** | **host** [*radius-server-name*]}

Syntax Description

attribute	Displays the H3C client version in the RADIUSRADIU server.
config-attribute	Displays the configured vendor-se RADIUS attribute information.
host	Displays RADIUS host configurat RADIUS servers.
host *radius-server-name*	Displays RADIUS host configurat specified RADIUS server.

Command Modes

Privileged EXEC (#)
Global Configuration (config)

Example

This example shows the sample output for the **show radius host** command:

```
Device> enable
Device# configure terminal
Device(config)# show radius host
------------------------------------------------------------------------

ServerName  = binidng
PrimAuthServerIP = 0.0.0.0          PrimAcctServerIP = 0.0.0.0
SecAuthServerIP  = 0.0.0.0          SecAcctServerIP  = 0.0.0.0
PrimAuthPort     = 1812             PrimAcctPort     = 1813
SecAuthPort      = 1812             SecAcctPort      = 1813
Auth-secretKey  = Switch        Acct-secretKey  = Switch
UserNameFormat = with-domain
RealTimeAcctSwitch = open       RealTimeAcctTime = 12
RadiusClientIP  = 0.0.0.0
------------------------------------------------------------------------
ServerName  = r1
PrimAuthServerIP = 0.0.0.0          PrimAcctServerIP = 0.0.0.0
SecAuthServerIP  = 0.0.0.0          SecAcctServerIP  = 0.0.0.0
PrimAuthPort     = 1812             PrimAcctPort     = 1813
SecAuthPort      = 1812             SecAcctPort      = 1813
Auth-secretKey  = Switch        Acct-secretKey  = Switch
UserNameFormat = with-domain
RealTimeAcctSwitch = open       RealTimeAcctTime = 12
RadiusClientIP  = 0.0.0.0
------------------------------------------------------------------------
ServerName  = mmm
PrimAuthServerIP = 0.0.0.0          PrimAcctServerIP = 0.0.0.0
SecAuthServerIP  = 0.0.0.0          SecAcctServerIP  = 0.0.0.0
PrimAuthPort     = 1812             PrimAcctPort     = 1813
SecAuthPort      = 1812             SecAcctPort      = 1813
Auth-secretKey  = Switch        Acct-secretKey  = Switch
```

```
UserNameFormat = with-domain
RealTimeAcctSwitch = open       RealTimeAcctTime = 12
RadiusClientIP  = 0.0.0.0
--------------------------------------------------------------------------
ServerName  = eee
PrimAuthServerIP = 0.0.0.0          PrimAcctServerIP = 0.0.0.0
SecAuthServerIP  = 0.0.0.0          SecAcctServerIP  = 0.0.0.0
PrimAuthPort     = 1812             PrimAcctPort     = 1813
SecAuthPort      = 1812             SecAcctPort      = 1813
Auth-secretKey  = Switch        Acct-secretKey  = Switch
UserNameFormat = with-domain
RealTimeAcctSwitch = open       RealTimeAcctTime = 12
RadiusClientIP  = 0.0.0.0
--------------------------------------------------------------------------
ServerName  = cisco
PrimAuthServerIP = 0.0.0.0          PrimAcctServerIP = 0.0.0.0
SecAuthServerIP  = 0.0.0.0          SecAcctServerIP  = 0.0.0.0
PrimAuthPort     = 1812             PrimAcctPort     = 1813
SecAuthPort      = 1812             SecAcctPort      = 1813
Auth-secretKey  = Switch        Acct-secretKey  = Switch
UserNameFormat = with-domain
RealTimeAcctSwitch = open       RealTimeAcctTime = 12
RadiusClientIP  = 0.0.0.0
--------------------------------------------------------------------------
ServerName  = 3
PrimAuthServerIP = 0.0.0.0          PrimAcctServerIP = 0.0.0.0
SecAuthServerIP  = 0.0.0.0          SecAcctServerIP  = 0.0.0.0
PrimAuthPort     = 1812             PrimAcctPort     = 1813
SecAuthPort      = 1812             SecAcctPort      = 1813
Auth-secretKey  = Switch        Acct-secretKey  = Switch
UserNameFormat = with-domain
RealTimeAcctSwitch = open       RealTimeAcctTime = 12
RadiusClientIP  = 0.0.0.0
--------------------------------------------------------------------------
ServerName  = radius1
PrimAuthServerIP = 0.0.0.0          PrimAcctServerIP = 10.1.1.10
SecAuthServerIP  = 0.0.0.0          SecAcctServerIP  = 0.0.0.0
PrimAuthPort     = 1812             PrimAcctPort     = 333
SecAuthPort      = 1812             SecAcctPort      = 1813
Auth-secretKey  = Switch        Acct-secretKey  = Switch
UserNameFormat = with-domain
RealTimeAcctSwitch = open       RealTimeAcctTime = 12
RadiusClientIP  = 0.0.0.0
--------------------------------------------------------------------------

Total [7] item(s), printed [7] item(s).
```

show shutdown-control interface

To display the shutdown configuration, use the **show shutdown-control interface** command in privileged EXEC or global configuration mode.

show shutdown-control interface [**ethernet** *slot-number/port-number* [**to ethernet** *slot-number/port-number*]]

Syntax Description

slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value • 10GE Ethernet: The valu • *port-number*: • GPON: The range is fro • GE Ethernet: The range • 10GE Ethernet: The rang
to	Displays the information for a rang the **to** keyword, specify the same p the keyword.

Command Modes

Privileged EXEC (#)
Global Configuration (config)

Example

This example shows a sample output for the **show shutdown-control interface** command:

```
Device> enable
Device# configure terminal
Device(config)# show shutdown-control interface
port shutdown control recover mode : manual
port shutdown control information :
PortID   Broadcast Broadcast Multicast Multicast Unicast Unicast
         status    value     status    value     status  value
e1/1     disable   -         disable   -         disable -
e1/2     disable   -         disable   -         disable -
e1/3     disable   -         disable   -         disable -
e1/4     disable   -         disable   -         disable -
e2/1     disable   -         disable   -         disable -
e2/2     disable   -         disable   -         disable -
Total entries: 6 .
```

show spanning-tree interface

To display the spanning tree configuration parameters, use the **show spanning-tree interface** command in the privileged EXEC and global configuration modes.

show spanning-tree interface [**brief** | {**ethernet** | **gpon**} *slot-number/port-number* [**to** {**ethernet** | **gpon**} *slot-number/port-number*]]

Syntax Description

slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1 • 10GE Ethernet: The value is • *port-number*: • GPON: The range is from 1 • GE Ethernet: The range is f • 10GE Ethernet: The range is
to	Displays the information for a range o the **to** keyword, specify the same port t the keyword.

Command Modes

Privileged EXEC (#)
Global Configuration (config)

Example

This example shows a sample output for the **show spanning-tree interface** command:

```
Device> enable
Device# configure terminal
Device(config)# show spanning-tree interface
Port g0/1 of bridge is Forwarding
   Spanning tree protocol is enabled
 Port g0/2 of bridge is DOWN
   Spanning tree protocol is enabled
 Port g0/3 of bridge is DOWN
   Spanning tree protocol is enabled
 Port g0/4 of bridge is DOWN
   Spanning tree protocol is enabled
 Port g0/5 of bridge is DOWN
   Spanning tree protocol is enabled
 Port g0/6 of bridge is DOWN
   Spanning tree protocol is enabled
 Port g0/7 of bridge is DOWN
   Spanning tree protocol is enabled
```

```
Port g0/8 of bridge is DOWN
  Spanning tree protocol is enabled
Port e1/1 of bridge is DOWN
  Spanning tree protocol is enabled
Port e1/2 of bridge is DOWN
  Spanning tree protocol is enabled
Port e1/3 of bridge is Forwarding
  Spanning tree protocol is enabled
Port e1/4 of bridge is DOWN
  Spanning tree protocol is enabled
Port e2/1 of bridge is DOWN
  Spanning tree protocol is enabled
Port e2/2 of bridge is DOWN
  Spanning tree protocol is enabled
```

shutdown-control-recover

To enable the port recovery mode and configure the port recovery parameters, use the **shutdown-control-recover** command in global configuration mode. To disable the port recovery mode and restore the default parameter values, use the **no** form of the command.

shutdown-control-recover {**automatic-open-time** *open-time* | **mode** {**automatic** | **manual**}}

no shutdown-control-recover {**automatic-open-time** | **mode**}

Syntax Description

automatic-open-time *open-time*	Configures the time after which the po recovery time is expires.
mode automatic	Enables automatic recovery mode.
mode manual	Enables manual recovery mode.

Command Modes

Global Configuration (config)

Example

This example shows how to configure automatic recovery mode on a port using the **shutdown-control-recover** command:

```
Device> enable
Device# configure terminal
Device(config)# shutdown-control-recover mode automatic
Device(config)#
```

spanning-tree (global configuration)

To enable spanning tree globally and configure the spanning tree parameters, use the **spanning-tree** command in global configuration mode. To disable spanning tree, use the **no** form of the command.

spanning-tree [**forward-time** *delay-time* | **hello-time** *hello-time* | **max-age** *age-time* | **mode** {**rstp** | **stp**} | **pathcost-standard** {**dot1d-1998** | **dot1t**} | **priority** *priority-value* | **root-guard action** {**block-port** | **drop-packets**}]

no spanning-tree [**forward-time** | **hello-time** | **max-age** | **mode** | **pathcost-standard** | **priority** | **root-guard action**]

Syntax Description

forward-time *delay-time*	Configures the forwarding delay o The range is 4 to 30 seconds.
hello-time *hello-time*	Configures the hello message time The range is 1 to 10 seconds.
max-age *age-time*	Configures the aging time of the s The range is 6 to 40 seconds.
mode rstp	Configures the RSTP spanning tre
mode stp	Configures the STP spanning tree
pathcost-standard dot1d-1998	Sets pathcost standard for dot1d-1
pathcost-standard dot1t	Sets pathcost standard for dot1t.
priority *priority-value*	Configures the switch priority. The range is from 0 to 61440, in s
root-guard action block-port	Enables root protection globally. BPDU configuration messages are packets are not forwarded.
root-guard action drop-packets	Enables root protection globally. BPDU configuration messages are packets are forwarded.

Command Modes

Global configuration (config)

Example

This example shows how to configure the forwarding delay of the system:

```
Device> enable
Device# configure terminal
```

```
Device(config)# spanning-tree forward-time 10
Device(config)#
```

Example

This example shows how to configure the hello message time interval:

```
Device> enable
Device# configure terminal
Device(config)# spanning-tree hello-time 5
Device(config)#
```

Example

This example shows how to configure the aging time of the system:

```
Device> enable
Device# configure terminal
Device(config)# spanning-tree max-age 10
Device(config)#
```

Example

This example shows how to configure RSTP spanning tree mode:

```
Device> enable
Device# configure terminal
Device(config)# spanning-tree mode rstp
Device(config)#
```

Example

This example shows how to configure STP spanning tree mode:

```
Device> enable
Device# configure terminal
Device(config)# spanning-tree mode stp
Device(config)#
```

Example

This example shows how to configure the pathcost standard:

```
Device> enable
Device# configure terminal
Device(config)# spanning-tree pathcost-standard dot1t
Device(config)#
```

Example

This example shows how to configure the switch priority:

```
Device> enable
Device# configure terminal
```

```
Device(config)# spanning-tree priority 3
Device(config)#
```

Example

This example shows how to enable root guard protection globally and configure the data packets to not be forwarded:

```
Device> enable
Device# configure terminal
Device(config)# spanning-tree root-guard action block-port
Device(config)#
```

spanning-tree (interface configuration)

To enable spanning tree on a specific interface and configure the spanning tree parameters, use the **spanning-tree** command in interface configuration mode. To disable spanning tree, use the **no** form of the command.

spanning-tree [**cost** *cost-value* | **loop-guard** | **mcheck** | **point-to-point** {**auto** | **forcefalse** | **forcetrue**} | **port-priority** *priority-value* | **portfast** | **root-guard** | **transit-limit value**]

no spanning-tree [**cost** | **loop-guard** | **point-to-point** | **port-priority** | **portfast** | **root-guard** | **transit-limit**]

Syntax Description

cost *cost-value*	Modifies the path cost of the STP por The range is 1 to 200000000.
loop-guard	Enables loop-guard on the port.
mcheck	Configures Mcheck on the port.
point-to-point auto	STP decides the point to point link.
point-to-point forcetrue	Enables the point to point link.
point-to-point forcefalse	Disables the point to point link.
port-priority *priority-value*	Configures the STP priority of the por The range is 0 to 240.
portfast	Configures the port as an edge port.
root-guard	Enables root protection locally on the
transit-limit *value*	Configures the port to send the maxim messages. The range is 1 to 255.

Command Modes

Interface configuration (config-if)

Example

This example shows how to configure the path cost of an STP port:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/3
Device(config-if-ethernet-1/3)# spanning-tree cost 1000
Device(config-if-ethernet-1/3)#
```

Example

This example shows how to enable loop guard on an STP port:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/3
Device(config-if-ethernet-1/3)# spanning-tree loop-guard
Device(config-if-ethernet-1/3)#
```

Example

This example shows how to configure Mcheck on an STP port:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/3
Device(config-if-ethernet-1/3)# spanning-tree mcheck
Device(config-if-ethernet-1/3)#
```

Example

This example shows how to enable point to point link on an STP port:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/3
Device(config-if-ethernet-1/3)# spanning-tree point-to-point forcetrue
Device(config-if-ethernet-1/3)#
```

Example

This example shows how to configure the STP priority of an STP port:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/3
Device(config-if-ethernet-1/3)# spanning-tree port-priority 3
Device(config-if-ethernet-1/3)#
```

Example

This example shows how to configure the STP port as an edge port:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/3
Device(config-if-ethernet-1/3)# spanning-tree portfast
Device(config-if-ethernet-1/3)#
```

Example

This example shows how to enable root protection on an STP port:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/3
Device(config-if-ethernet-1/3)# spanning-tree root-guard
Device(config-if-ethernet-1/3)#
```

Example

This example shows how to configure an STP port to send the maximum rate of BPDU messages:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/3
Device(config-if-ethernet-1/3)# spanning-tree transit-limit 200
Device(config-if-ethernet-1/3)#
```

time-range

To specify when an access control list (ACL) is in effect, use the **time-range** command in the global configuration mode. To remove the time range, use the **no** form of the command.

```
[no]time-range name
```

Syntax Description

name	Specifies a unique name for the time range. Name has to begin with an alphabetic character.

Command Modes

Global Configuration (config)

Command Default

None

Example

```
Device#configure terminal
Device(config)#time-range weekends
```

username-format

To configure a packet to carry the username when it is passed by the system to the RADIUS server, use the **username-format** command in AAA configuration module.

username-format {**with-domain** | **without-domain**}

Syntax Description

with-domain	Configures the packet to carry the use domain.
without-domain	Configures the packet to carry the use domain.

Command Modes

AAA configuration (config-aaa)

Example

This example shows how to configure the system to carry the user name when it passes a packet to the RADIUS server using the **username-format** command:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius host radius1
Device(config-aaa-radius-radius1)# username-format with-domain
 Modify the username format of RADIUS configuration successfully
```

PART VIII

Multicast Configuration

Multicast Configuration

igmp-snooping

To enable IGMP Snooping, use the **igmp-snooping** command in the global configuration mode. To disable IGMP Snooping, use the **no** form of the command.

igmp-snooping

no igmp-snooping

Syntax Description

igmp-snooping	Enables IGMP Snooping.

Command Default

IGMP Snooping is enabled by default.

Command Modes

Global configuration

Examples

The following example shows how to enable IGMP Snooping.

```
Device(config)#igmp-snooping
```

igmp-snooping drop

To configure a port to drop query or report packets, use the **igmp-snooping drop** command in the interface configuration mode. To configure the port to start receiving IGMP query or report packets, use the **no** form of the command.

igmp-snooping drop {**query** | **report**}

no igmp-snooping drop

Syntax Description

query	Configures the port to drop IGMP query packets.
report	Configures the port to drop IGMP report packets.

Command Default

Packet dropping is not enabled by default.

Command Modes

Interface configuration

Examples

The following example shows how to comfigure a port to drop query packets:

```
Device(config-if-ethernet-1/1)# igmp-snooping drop query
```

igmp-snooping fast-leave

To remove the port directly from the multicast group upon receiving an IGMP Leave message, use the **igmp-snooping fast-leave** command in the interface configuration mode. To disable fast leave use the **no** form of the command.

igmp-snooping fast-leave

no igmp-snooping fast-leave

Syntax Description

fast-leave	Removes the port directly from the multicast group upon receiving an IGMP Leave message

Command Default

Fast leave is not configured by default.

Command Modes

Interface configuration

Examples

The following example shows how to configure fast leave:

```
Device(config-if-ethernet-1/1)#igmp-snooping fast-leave
```

igmp-snooping group-limit action

To configure the action that the port will perform when it reaches the maximum number of multicast groups it can join, use the **igmp-snooping group-limit action** command in the interface configuration mode.

igmp-snooping group-limit action {**drop** | **replace**}

Syntax Description

drop	Drops the multicast group. This is the default action.
replace	Replaces an old multicast group with the new group.

Command Default

When the group limit is reached, the new group is dropped.

Command Modes

Interface configuration

Examples

This example shows how to configure the port to drop new multicast groups when it reaches the group limit

```
Device(config-if-ethernet-1/1)#igmp-snooping group-limit action drop
```

igmp-snooping group-limit

To configure the maximum number of multicast groups that an interface or a port can learn or join, use the **igmp-snooping group-limit** command in the interface configuration mode. To undo the limit on the maximum number of multicast groups that a port can join use the **no** form of the command.

igmp-snooping group-limit *number*

no igmp-snooping group-limit

Syntax Description

number	Specifies the maximum number of multicast groups that a port can join.The range is 0-1024.

Command Default

No limit is configured by default.

Command Modes

Interface configuration

Examples

The following examples shows how to configure a group limit of 100:

```
Device(config-if-ethernet-1/4)#igmp-snooping group-limit 100
```

igmp-snooping general-query source-ip

To configure the source IP address for sending general query packets, use the **igmp-snooping general-query source-ip** command in the global configuration mode. To disable the source IP address for sending general query, use the **no** form of the command.

igmp-snooping general-query source-ip*ip-address*

no igmp-snooping general-query source-ip*ip-address*

Syntax Description

ip-address	Configures the source IP address for sending general query packets.

Command Default

None

Command Modes

Global configuration

Examples

The following example shows how to configure a source IP address for sending general query packets:

```
Device(config)# igmp-snooping general-query source-ip 192.168.1.2
```

igmp-snooping host-aging-time

To configure the aging time of dynamic multicast members, use the **igmp-snooping host-aging-time** command in the global configuration mode. To disable aging time for dynamic multicast members use the **no** form of the command.

igmp-snooping host-aging-time*time*

no igmp-snooping host-aging-time

Syntax Description

time	Specifies the aging time for dynamic multicast members. The range is from 10-1000000 seconds. The default value is 300 seconds.

Command Default

The aging time is set to 300 seconds.

Command Modes

Global configuration

Examples

The following example shows how to configure an aging time of 500 seconds:

```
Device(config)# igmp-snooping host-aging-time 500
```

igmp-snooping max-response-time

To configure the maximum waiting time for deleting group ports after receiving a leave packet, use the **igmp-snooping max-resposne-time** command in the global configuration mode.To disable a maximum waiting time use the **no** form of the command.

igmp-snooping max-response-time *time*

no igmp-snooping max-response-time *time*

Syntax Description

time	Configures the maximum waiting time for deleting group ports after receiving a leave packet. The range is from 1-100 seconds. The default value is 10 seconds.

Command Default

The default maximum waiting time is 10 seconds.

Command Modes

Global configuration

Examples

The following example shows how to configure a maximum response time of 20 seconds:

```
Device(config)# igmp-snooping max-response-time 20
```

igmp-snooping multicast vlan

To configure multicast VLAN for IGMP packets, use the **igmp-snooping multicast vlan** command in the interface configuration mode. To disable multicast VLAN for IGMP packets, use the **no** form of the command.

igmp-snooping multicast vlan *vlan-id*

no igmp-snooping multicast vlan

Syntax Description

multicast vlan	Configures multicast VLAN for the IGMP packets on the port.

Command Default

None

Command Modes

Interface configuration

Examples

The following example shows how to enable multicast VLAN for IGMP packets on VLANs 1-50:

```
Device(config-if-ethernet-1/1)# igmp-snooping multicast vlan 50
```

igmp-snooping {permit|deny}

To configure the default learning rule for multicast groups that are not in the blocked list or the allowed list, use the **igmp-snooping {permit|deny}** command in the global configuration mode. By default, the learning rule for all multicast groups that are not in the blocked list or the allowed list is to learn all multicast groups.

igmp-snooping {**permit** | **deny**} {**group all** | **vlan***vlan-id*

Syntax Description

permit	Configures the list of groups that are permitted to join by IGMP snooping.
deny	Configures the list of groups that are denied to join by IGMP snooping.

Command Default

Default is to learn all multicast groups that are not in the blocked list or the allowed list

Command Modes

Global configuration

Examples

This example shows how to configure the rule to learn all multicast groups:

```
Device(config)#igmp-snooping permit group all
```

igmp-snooping profile refer

To configure a profile or a list of profiles as a reference for a port, use the **igmp-snooping profile refer** command in the interface configuration mode. You can disable the profile reference of a port using the **no** form of the command.

igmp-snooping profile refer*profile-list*

no igmp-snooping profile refer*profile-list*

Syntax Description

profile-list	Configures a list of reference profiles for the port.

Command Default

None

Command Modes

Interface configuration

Examples

The following exaple shows how to create reference profile for the port:

```
Device(config-if)# igmp-snooping profile refer 1-5
```

igmp-snooping profile

To create an IGMP Snooping profile, use the **igmp-snooping profile** command in the global configuration mode. To disable IGMP snooping profile use the **no** form of the command.

igmp-snooping profile *profile-id*

no igmp-snooping profile

Syntax Description

profile-id	Functions as an identifier for an IGMP Snooping profile. The range is 1-128.

Command Default

IGMP Snooping profile is not enabled by default.

Command Modes

Global configuration

Examples

The following example shows how to create an IGMP Snooping profile:

```
Device(config)# igmp-snooping profile 1
```

igmp-snooping {permit|deny} group-range

To configure a port to learn (or not learn) a range of MAC addresses and VLAN ids, use the **igmp-snooping {permit|deny} group-range** command in the interface configuration mode.

igmp-snooping { **permit** | **deny** } **group-range** *MAC-address* **multi-count** *multi-count-number***vlan** *vlan-list*

Syntax Description

multi-count *multi-count-number*	Configures the number of MAC addresses in the group range.

Command Default

None

Command Modes

Interface configuration

Examples

The following example shows how to permit a group range of MAC addresses and VLAN ids:

```
Device(config-if-ethernet-1/1)# igmp-snooping permit group-range 01:00:5e:09:08:07 multi-count
 12 vlan 10
```

igmp-snooping query-interval

To configure the interval for sending general query packets, use the **igmp-snooping query-interval** command in the global configuration mode.

igmp-snooping query-interval *interval*

Syntax Description

interval	Configures the interval for sending general query packets. The range is from 1 to 30000 seconds.

Command Default

None

Command Modes

Global configuration

Examples

The following example shows how to configure the IGMP Snooping query interval to 500 seconds:

```
Device(config)# igmp-snooping query-interval 500
```

igmp-snooping querier version

To configure the version of the IGMP Snooping querier, use the **igmp-snooping querier version** command in the global configuration mode. The IGMP snooping querier version is set to 2 by default.

igmp-snooping querier version *version-id*

Syntax Description

version-id	Configures the version of the IGMP Snooping querier. The range is 2-3. The default version is 2.

Command Default

the querier is set to version 2 by default.

Command Modes

Global configuration

Examples

The following example shows how to configure the IGMP Snooping querier vesion to version 3:

```
Device(config)# igmp-snooping querier version 3
```

igmp-snooping querier-vlan

To configure VLANs for general query packets, use the **igmp-snooping querier-vlan** command in the global configuration mode. To disable VLANs for query packets use the **no** form of the command.

igmp-snooping querier-vlan*vlan-list*

no igmp-snooping querier-vlan*vlan-list*

Syntax Description

querier-vlan	Configures a list of VLANs for general query packets.

Command Default

None

Command Modes

Global configuration

Examples

The following example shows how to configure VLANs for the IGMP-Snooping querier:

```
Device(config)# igmp-snooping querier-vlan 1-50
```

igmp-snooping query-max-respond

To configure the maximum response time for general query packets, use the **igmp-snooping query-max-respond** command in the global configuration mode. To disable a maximum response time, use the **no** form of the command.

igmp-snooping query-max-respond *time*

no igmp-snooping query-max-respond *time*

Syntax Description

time	Configures the maximum response time for general query packets. The range is from 1 to 25 seconds.

Command Default

None

Command Modes

Global configuration

Examples

The following example shows how to configure the maximum response time for general query packets to 10 seconds:

```
Device(config)# igmp-snooping query-max-respond 10
```

igmp-snooping record-host

To enable recording the MAC address of the source of an IGMP report packet, use the **igmp-snooping record-host** command in the interface configuration mode. To disable the recording of the host MAC address, use the **no** form of the command.

igmp-snooping record-host

no igmp-snooping record-host

Syntax Description

record-host	Enables recording the MAC address of the source of an IGMP report packet

Command Default

recording is not enabled by default

Command Modes

Interface configuration

Examples

The following example shows how to configure a port to record the host MAC address

```
Device(config-if-ethernet-1/1)# igmp-snooping record-host
```

igmp-snooping router-port-age

To configure the ageing time for the dynamic route port, use the **igmp-snooping router-port-age** command in the global configuration mode. To disable ageing time for the dynamic route port, use the **no** form of the command.

igmp-snooping router-port-age {**on** | **off** | *age-time*}

no igmp-snooping router-port-age {**on** | **off** | *age-time*}

Syntax Description

on	Starts router port age
off	Stops router port age.
age-time	Sets router port age time in seconds. The range is 10-1000000 seconds. The default value is 300 seconds.

Command Default

The router port age is on by default.

Command Modes

Global configuration

Examples

The following example shows how to start the rotuter port age:

```
Device(config)# igmp-snooping router-port-age on
```

igmp-snooping route-port forward

To configure a dynamic route port to forward multicast traffic packets, use the **igmp-snooping route-port forward** command in the global configuration mode. To disable the route port from forwarding multicast traffic packets, use the **no** form of the command.

igmp-snooping route-port forward

no igmp-snooping route-port forward

Syntax Description

forward	Configures the port to forward multicast traffic packets.

Command Default

None

Command Modes

Global configuration

Examples

The following example shows how to configure a dynamic route port to forward multicast traffic packets:

```
Device(config)# igmp-snooping route-port forward
```

igmp-snooping report-supression

To enable IGMP Snooping supression of multicast reports, use the **igmp-snooping report-supression** command in the global configuration mode. To disable the suppression of multicast reports, use the **no** form of the command.

igmp-snooping report-supression

no igmp-snooping report-supression

Syntax Description

report-supression	Enables IGMP Snooping supression of multicast reports.

Command Default

Report supression is not enabled by default.

Command Modes

Global configuration

Examples

The following example shows how to enable IGMP Snooping report supression:

```
Device(config)# igmp-snooping report-suppression
```

igmp-snooping route-port vlan

To configure a static route port, use the **igmp-snooping route-port vlan** command in the global configuration mode. You can disable the static route port by using the **no** form of the command.

igmp-snooping route-port vlan *vlan-id* **interface** {**all** | **channel-group** *channel-group-id* | **ethernet** *interface-number*

no igmp-snooping route-port vlan *vlan-id* **interface** {**all** | **channel-group** *channel-group-id* | **ethernet** *interface-number*

Syntax Description

channel-group-id	Specifies the number of the channel group. The range is from 0-5.
interface-number	Specifies the ethernet interface number.

Command Default

None.

Command Modes

Global configuration

Examples

The following examples shows how to configure all the ports of an interface as static route ports:

```
Device(config)# igmp-snooping route-port vlan 50 interface all
```

ip range

To configure the range of IP addresses and VLAN IDs for an IGMP profile, use the **ip range** command in profile configuration mode.

ip range *start-ip-address end-ip-address* **vlan** *vlan-id*

Syntax Description

start-ip-address	Configures the start IP Address for the IGMP Snooping profile. The IP addresses range is from 224.0.0.1 to 239.255.255.254.
end-ip-address	Configures the end IP Address for the IGMP Snooping profile.The IP addresses range is from 224.0.0.1 to 239.255.255.254.
vlan-id	Configures the range of VLAN IDs for the IGMP Snooping profile. The VLAN id range is from 1 to 4094.

Command Default

None

Profile configuration mode

Examples

The following example shows how to configure the range of IP addresses and VLAN ids for an IGMP Snooping profile.

```
Device(config-igmp-profile-1)# ip range 224.0.0.1 239.255.255.254 vlan 50
```

mac range

To configure the range of MAC addresses and VLAN IDs for an IGMP profile, use the **mac range** command in profile configuration mode.

mac range *start-mac-address end-mac-address* **vlan** *vlan-id*

Syntax Description

start-mac-address	Configures the start MAC Address for the IGMP Snooping profile. The MAC addresses range is 01:00:5e:H:H:H. .
end-mac-address	Configures the end MAC Address for the IGMP Snooping profile.The MAC addresses range is 01:00:5e:H:H:H.
vlan-id	Configures the range of VLAN IDs for the IGMP Snooping profile. The VLAN id range is from 1 to 4094.

Command Default

None

Command Modes

Profile configuration

Examples

The following example shows how to configure the range of MAC addresses and VLAN ids for an IGMP Snooping profile.

```
Device(config-igmp-profile-1)# mac range 01:00:5e:09:08:07 01:00:5e:09:09:08 vlan 50
```

mld-snooping

To enable MLD Snooping, use the **mld-snooping** command in the global configuration mode. To disable MLD Snooping, use the **no** form of the command.

mld-snooping

no mld-snooping

Command Default

MLD Snooping is disabled by default.

Command Modes

Global configuration

Examples

The following example shows how to enable MLD Snooping.

```
Device(config)# mld-snooping
```

mld-snooping fast-leave

To remove the port directly from the multicast group upon receiving a Leave message, use the **mld-snooping fast-leave** command in the interface configuration mode. To disable fast leave, use the **no** form of the command.

Command Default

Fast leave is not configured by default.

Command Modes

Interface configuration

Examples

The following example shows how to configure fast leave:

```
Device(config-if-ethernet-1/1)# mld-snooping fast-leave
```

mld-snooping group-limit

To configure the maximum number of IPv6 multicast groups that an interface or a port can learn or join, use the **mld-snooping group-limit** command in the interface configuration mode. To undo the limit on the maximum number of IPv6 multicast groups that a port can join use the **no** form of the command.

mld-snooping group-limit *number*

no mld-snooping group-limit

Syntax Description

number	Specifies the maximum number of IPv6 multicast groups that a port can join.The range is 0-1024.

Command Default

No limit is configured by default.

Command Modes

Interface configuration

Examples

The following example shows how to configure a group limit of 100:

```
Device(config-if-ethernet-1/4)# mld-snooping group-limit 100
```

mld-snooping host-aging-time

To configure the aging time of dynamic multicast ports, use the **mld-snooping host-aging-time** command in the global configuration mode. To disable aging time for dynamic multicast ports use the **no** form of the command.

mld-snooping host-aging-time *time*

no mld-snooping host-aging-time

Syntax Description

time	Specifies the aging time for dynamic multicast ports. The range is from 10-1000000 seconds. The default value is 300 seconds.

Command Default

The aging time is set to 300 seconds.

Command Modes

Global configuration

Examples

The following example shows how to configure an aging time of 500 seconds for a host:

```
Device(config)# mld-snooping host-aging-time 500
```

mld-snooping max-response-time

To configure the maximum response time of the leave packets, use the **mld-snooping max-resposne-time** command in the global configuration mode. To disable the maximum response time, use the **no** form of the command.

mld-snooping max-response-time *time*

no mld-snooping max-response-time *time*

Syntax Description

time	Configures the maximum waiting time to send a response after receiving a leave packet. The range is from 1-100 seconds. The default value is 10 seconds.

Command Default

The default maximum waiting time is 10 seconds.

Command Modes

Global configuration

Examples

The following example shows how to configure a maximum response time of 20 seconds:

```
Device(config)# mld-snooping max-response-time 20
```

mld-snooping multicast vlan

To configure multicast VLAN with MLD snooping, use the **mld-snooping multicast vlan** command in the global configuration mode.

mld-snooping multicast vlan *vlan_id*

Syntax Description

vlan_id	The VLAN ID. The range is from 1 to 4094.

Command Default

None

Command Modes

Interface configuration (config-if)

Examples

This example shows how to configure multicast VLAN with MLD snooping:

```
Device> enable
Device# configure terminal
Device(config)# interface gpon 0/1
Device(config-if-gpon-0/1)# mld-snooping multicast vlan 1
```

mld-snooping {permit|deny} {group|vlan}

To specify a learning rule on the device for the multicast groups that are not part of a blocked list or an allowed list, use the **mld-snooping** { **permit** | **deny** } { **group** | **vlan** } command in the global configuration mode.

mld-snooping { **permit** | **deny** } { **group all** | **vlan** *vlan-list* }

Syntax Description

group all	Specifies that the learning policy applies to all multicast groups.
vlan *vlan-list*	Specifies the VLAN to which the learning policy applies.

Command Default

None

Command Modes

Global configuration

Examples

The following example shows how to permit the learning rule for all multicast groups.

```
Device(config)# mld-snooping permit group all
```

mld-snooping permit deny group MAC vlan

To configure a list of multicast groups that are permitted or denied by MLD snooping in a particular VLAN, use the **mld-snooping** { **permit** | **deny**} **group** *MAC* **vlan** *vlan-id* in the interface configuration mode.

mld-snooping { **permit** | **deny** } **group** *MAC-address* **vlan** *vlan-id*

Syntax Description

MAC-address	Specifies the list of multicast groups that start at the *MAC-address*

Command Default

None

Command Modes

Interface configuration

Examples

The following example shows how to permit a group of MAC addresses in VLAN 5:

```
Device(config-if-ethernet-1/1)# mld-snooping permit group 33:33:5e:09:08:07 vlan 5
```

mld-snooping {permit|deny} group-range

To configure a port to learn (or not learn) a range of MAC addresses and VLAN ids, use the **mld-snooping {permit|deny} group-range** command in the interface configuration mode.

mld-snooping { **permit** | **deny** } **group-range** *MAC-address* **multi-count** *multi-count-number* **vlan** *vlan-list*

Syntax Description

multi-count *multi-count-number*	Configures the number of MAC addresses in the group range.

Command Default

None

Command Modes

Interface configuration

Examples

The following example shows how to permit a group range of MAC addresses and VLAN ids:

```
Device(config-if-ethernet-1/1)# mld-snooping permit group-range 33:33:5e:09:08:07 multi-count
 12 vlan 10
```

mld-snooping querier

To enable MLD Snooping querier to forward the source address, maximum response time, and query interval for sending general query messages, use the **mld-snooping querier** command in the global configuration mode. To disable MLD Snooping querier, use the **no** form of the commnd.

mld-snooping querier

Command Default

MLD Snooping querier is disabled by default.

Command Modes

Global configuration

Examples

The following example shows how to enable MLD Snooping querier :

```
Device(config)# mld-snooping querier
```

mld-snooping querier-vlan

To configure VLANs for general query packets, use the **mld-snooping querier-vlan** command in the global configuration mode. To disable VLANs for query packets use the **no** form of the command.

mld-snooping querier-vlan *vlan-id*

no mld-snooping querier-vlan *vlan-id*

Syntax Description

vlan-id	Specifes the VLAN that carries the general query packets. The range is 1 to 4094.

Command Default

None

Command Modes

Global configuration

Examples

The following example shows how to configure a VLAN for the MLD Snooping querier:

```
Device(config)# mld-snooping querier-vlan 50
```

mld-snooping query-interval

To configure the interval for sending mld snooping general query packets, use the **mld-snooping query-interval** command in the global configuration mode.

mld-snooping query-interval *interval*

Syntax Description

interval	Configures the interval for sending mld-snooping general query packets. The range is from 1 to 30000 seconds.

Command Default

None

Command Modes

Global configuration

Examples

The following example shows how to configure the MLD Snooping query interval to 3000 seconds:

```
Device(config)# mld-snooping query-interval 3000
```

mld-snooping query-max-respond

To configure the maximum response time for general query packets, use the **mld-snooping query-max-respond** command in the global configuration mode. To disable a maximum response time, use the **no** form of the command

mld-snooping query-max-respond *time*

no mld-snooping query-max-respond *time*

Syntax Description

time	Configures the maximum response time for general query packets. The range is from 1 to 25 seconds.

Command Default

None

Command Modes

Global configuration

Examples

The following example shows how to configure the maximum response time for general query packets to 10 seconds:

```
Device(config)# mld-snooping query-max-respond 10
```

mld-snooping route-port forward

To configure a dynamic route port to forward IPv6 multicast traffic packets, use the **mld-snooping route-port forward** command in the global configuration mode. To disable the route port from forwarding IPv6 multicast traffic packets, use the **no** form of the command.

mld-snooping route-port forward

no igmp-snooping route-port forward

Syntax Description

forward	Configures the port to forward IPv6 multicast traffic packets.

Command Default

None

Command Modes

Global configuration

Examples

The following example shows how to configure a dynamic route port to forward IPv6 multicast traffic packets:

```
Device(config)# mld-snooping route-port forward
```

mld-snooping route-port vlan

To configure a mutlicast router VLAN and specify the interface to the multicast router, use the **mld-snooping route-port vlan** command in the global configuration mode. You can disable the mutlicast router VLAN by using the **no** form of the command.

mld-snooping route-port vlan *vlan-id* **interface** { **all** | **ethernet** *interface-number*

no mld-snooping route-port vlan *vlan-id* **interface** { **all** | **ethernet** *interface-number*

Syntax Description

all	Specifies that all ports are multicast router interfaces.
ethernet *interface-number*	Specifies the ethernet interface number.

Command Default

None.

Command Modes

Global configuration

Examples

The following examples shows how to configure all the ports of an interface as multicast route ports:

```
Device(config)# mld-snooping route-port vlan 50 interface all
```

mld-snooping router-port-age

To configure the ageing time for the dynamic route port, use the **mld-snooping router-port-age** command in the global configuration mode. To disable ageing time for the dynamic route port, use the **no** form of the command.

mld-snooping router-port-age { **on** | **off** | *age-time* }

no mld-snooping router-port-age { **on** | **off** | *age-time* }

Syntax Description

on	Starts router port age
off	Stops router port age.
age-time	Sets router port age time in seconds. The range is 10-1000000 seconds. The default value is 300 seconds.

Command Default

The router port age is on by default.

Command Modes

Global configuration

Examples

The following example shows how to start the router port age:

```
Device(config)# mld-snooping router-port-age on
```

mld-snooping record-host

To enable the port to record the host information, use the **mld-snooping record-host** command in the global configuration mode.

mld-snooping record-host

Command Default

None

Command Modes

Interface configuration (config-if)

Examples

This example shows how to enable the port to record the host information:

```
Device> enable
Device# configure terminal
Device(config)# interface gpon 0/1
Device(config-if-gpon-0/1)# mld-snooping record-host
```

multicast

To create a static multicast group, use the **multicast** command in the global configuration mode.

multicast { **mac-address***mac-address* | **ip-address** *ip-address* } **vlan** *vlan-id*

Syntax Description

ip-address	Configures the static multicast IP address. It can only be in the format 224.x.x.x.
mac-address	Configures the static multicast MAC address. It can only be in the format 01:00:5e:H:H:H.
vlan-id	Configures the VLANS for the static multicast group.

Command Default

Multicast group is not configured by default.

Command Modes

Global configuration

The following example shows how to configure a static multicast group:

```
Device(config)# multicast ip-address 224.0.0.3 vlan  50
Adding multicast group successfully !
```

multicast ds-tag add

To configure the ONT downlink multicast VLAN tag adding rule, use the **multicast ds-tag add** command in line profile configuration mode.

To disable the ONT uplink multicast VLAN tag adding rule, use the **no multicast ds-tag add** command.

multicast ds-tag add *vlan_id* {*priority* | **port** *port_id*}

no multicast ds-tag port *port_id*

Syntax Description

vlan_id	The VLAN ID The range is from 1 to 4094.
priority	The 802.1 priority value. The range is from 0 to 7.
port_id	The ONT Ethernet port ID. The range is from 1 to 24.

Command Modes

Line profile configuration (deploy-profile-line)

Examples

This example shows how to configure the ONT downlink multicast VLAN tag adding rule.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 5
Device(deploy-profile-line-5)# multicast ds-tag add 3
```

multicast ds-tag remove

To configure the ONT downlink multicast VLAN tag removing rule, use the **multicast ds-tag remove port** command in line profile configuration mode. To delete the ONT downlink multicast VLAN tag, use the **no multicast ds-tag port** command

multicast ds-tag remove [**port** *port_id*]

no multicast ds-tag [**port** *port_id*]

Syntax Description

port_id	The ONT Ethernet port ID. The range is from 1 to 24.

Command Modes

Line profile configuration (deploy-profile-line)

Examples

This example shows how to configure the ONT downlink multicast VLAN tag removing rule.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 5
Device(deploy-profile-line-5)# multicast ds-tag remove
```

multicast ds-tag translate

To configure the ONT downlink multicast VLAN tag translating rule, use the **multicast ds-tag translate** command in line profile configuration mode.

multicast ds-tag translate *vlan_id* [*priority* | **port** *port_id*]

Syntax Description

vlan_id	The VLAN ID The range is from 1 to 4094.
priority	The 802.1 priority value. The range is from 0 to 7.
port_id	The ONT Ethernet port ID. The range is from 1 to 24.

Command Modes

Line profile configuration (deploy-profile-line)

Usage Guidelines

You must configure a device type.

Examples

This example shows how to configure the ONT downlink multicast VLAN tag translating rule.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 5
Device(deploy-profile-line-5)# multicast ds-tag translate 3
```

multicast fast-leave disable

To disable fast-leave, use the **multicast fast-leave disable** command in global configuration mode.

multicast fast-leave disable [**port** *port_id*]

no multicast fast-leave disable [**port** *port_id*]

Syntax Description

port_id	The ONT Ethernet port ID. The range is from 1 to 24.

Command Modes

Line profile configuration (deploy-profile-line)

Examples

This example shows how to disable fast-leave on a port.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 5
Device(deploy-profile-line-5)# multicast fast-leave disable
```

multicast group-limit

To configure the limit of multicast groups, use the **multicast group-limit** *limit_number* command in line profile configuration mode. To disable the limit of multicast groups, use the **no multicast group-limit** *limit_number* command.

multicast group-limit *limit_number* [**port** *port_id*]

no multicast group-limit *limit_number* [**port** *port_id*]

Syntax Description

limit_number	The multicast group limit. The range is fro
port_id	The ONT Ethernet port ID. The range is fr

Command Modes

Line profile configuration (deploy-profile-line)

Examples

This example shows how to configure the limit of multicast groups.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 5
Device(deploy-profile-line-5)# multicast group-limit 4
```

multicast interface

To add a port to a static multicast group, use the **multicast interface** command in the global configuration mode.

multicast { **mac-address***mac-address* | **ip-address** *ip-address* } **vlan** *vlan-id***interface** { **all** | *interface-list* }

Syntax Description

all	Adds all the ports of the interface to the static multicast group.
interface-list	Adds the specified ports of the interface to the static multicast group.

Command Default

None.

Command Modes

Global configuration

The following example shows how to add all the ports of an interface to a static multicast group:

```
Device(config)# multicast ip-address 224.0.0.11
vlan 1 interface all
```

multicast mode igmp-snooping

To enable Internet Group Management Protocol (IGMP) snooping, use the **multicast mode igmp-snooping** command in line profile configuration mode.

multicast mode igmp-snooping [**port** *port_id*]

Syntax Description

port_id	The ONT Ethernet port ID. The range is from 1 to

Command Modes

Line profile configuration (deploy-profile-line)

Examples

This example shows how to enable IGMP snooping on a port.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 5
Device(deploy-profile-line-5)# multicast mode igmp-snooping port 10
```

multicast proxy-interval

To configure the interval at which the device sends report packets to the multicast source through the proxy port, use the **multicast proxy-inteval** command in the global configuration mode.

multicast proxy-interval *seconds*

Syntax Description

proxy-interval	Configures the interval at which the device sends report packets to the multicast source through the proxy port.
seconds	Configures the proxy-interval in seconds. The range is from 1-300. The default is 10 seconds.

Command Default

The default interval is 10 seconds.

Command Modes

Global configuration

Example

The following example shows how to configure the proxy-interval to 100 seconds

```
Device(config)# multicast proxy-interval 100
```

multicast proxy-port

To configure a proxy-port for the static multicast group, use the **multicast proxy-port** command in the global configuration mode.

multicast { **mac-address***mac-address* | **ip-address** *ip-address* } **vlan** *vlan-id***proxy-port ethernet** *port-id*

Syntax Description

proxy-port	Configures a proxy port to send the multicast report to the multicast source.
port-id	Configures the port that will act as the proxy port.

Command Default

None

Command Modes

Global configuration

The following example shows how to configure a proxy port for a static multicast group:

```
Device(config)# multicast ip-address 225.0.0.11 vlan 1 proxy-port ethernet 1/1
```

multicast us-tag add

To configure the ONT uplink multicast VLAN tag adding rule, use the **multicast us-tag add** command in line profile configuration mode. To disable the ONT uplink multicast VLAN tag adding rule, use the **no multicast us-tag add** command.

multicast us-tag add *vlan_id* {*priority* | **port** *port_id*}

`no multicast us-tag port` *port_id*

Syntax Description

vlan_id	The VLAN ID The range is from 1 to 4094.
priority	The 802.1 priority value. The range is from 0 to 7.
port_id	The ONT Ethernet port ID. The range is from 1 to 24.

Command Modes

Line profile configuration (deploy-profile-line)

Examples

This example shows how to configure the ONT uplink multicast VLAN tag adding rule

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 5
Device(deploy-profile-line-5)# multicast us-tag add 3
```

multicast us-tag translate

To configure the ONT downlink multicast VLAN tag translating rule, use the **multicast us-tag translate** command in line profile configuration mode. To disable the ONT downlink multicast VLAN tag translating rule, use the **no multicast us-tag translate** command

multicast us-tag translate *vlan_id* {*priority* | **port** *port_id*}

no multicast us-tag port *port_id*

Syntax Description

vlan_id	The VLAN ID The range is from 1 to 4094.
priority	The 802.1 priority value. The range is from 0 to 7.
port_id	The ONT Ethernet port ID. The range is from 1 to 24.

Command Modes

Line profile configuration (deploy-profile-line)

Examples

This example shows how to configure the ONT uplink multicast VLAN tag translating rule.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 5
Device(deploy-profile-line-5)# multicast us-tag translate 3
```

profile limit

To configure the IGMP snooping profile type as a permit or deny profile, use the **profile limit** command in the profile configuration mode.

profile limit { **permit** | **deny** }

Syntax Description

permit	Configures a list of groups that are permitted by the IGMP Snooping profile.
deny	Configures a list of groups that are denied by the IGMP Snooping profile.

Command Default

None

Command Modes

Profile configuration

Examples

The folloiwng example shows how to configure a permit type profile:

```
Device(config-igmp-profile-1)# profile limit permit
```

show igmp-snooping

To displays IGMP Snooping configurations, use the **show igmp-snooping** command in the EXEC mode.

show igmp-snooping

Syntax Description

igmp-snooping	Displays IGMP Snooping configurations.

Command Default

None

Command Modes

User EXEC
Privileged EXEC

Examples

The following example shows the output from **show igmp-snooping** command on an inteface where IGMP SNooping is enabled:

```
Device# show igmp-snooping
Enable IGMP-Snooping
Disable IGMP-Snooping report-suppression
The max response time is 10 second(s)
The host aging time is 300 second(s).
Disable IGMP-Snooping route-port forward
The Router port timeout is 300 second(s), Currently aging is running
Denied VLAN:
Blocked list:
NULL
Allowed list:
NULL
Default group policy is permit
IGMP-Snooping Querier : ON
Querier vlan : 1
Querier Source IP 0.0.0.0 | Max Query Respond Time 10 sec | Query interval 60
sec | Igmp version 2
Port Information:
port  limit  action  fast-leave  mcast-vlan  igmp-profile  drop-type
p0/1  1024   drop    disabled    disabled    disabled      null
p0/2  1024   drop    disabled    disabled    disabled      null
p0/3  1024   drop    disabled    disabled    disabled      null
p0/4  1024   drop    disabled    disabled    disabled      null
p0/5  1024   drop    disabled    disabled    disabled      null
p0/6  1024   drop    disabled    disabled    disabled      null
p0/7  1024   drop    disabled    disabled    disabled      null
p0/8  1024   drop    disabled    disabled    disabled      null
e1/1  1024   drop    disabled    disabled    1             null
e1/2  1024   drop    disabled    disabled    disabled      null
e1/3  1024   drop    disabled    disabled    disabled      null
e1/4  1024   drop    disabled    disabled    disabled      null
e2/1  1024   drop    disabled    disabled    disabled      null
e2/2  1024   drop    disabled    disabled    disabled      null
```

show igmp-snooping profile

To display the details of an IGMP Snooping profile, use the **show igmp-snooping profile** command in the EXEC mode.

showigmp-snooping profile {*profile-id* | **interface** *port-id* | **vlan** *vlan-id*}

Syntax Description

profile-id	Displays the details of the particular IGMP Snooping profile
port-id	Displays the IGMP Snooping profile details for the port.
vlan-id	Displays the IGMP Snooping profile details for the VLANs.

Command Default

None

Command Modes

User EXEC
Privileged EXEC

Examples

The following example displays the output of the **show igmp-snooping profile** command:

```
Device# show igmp-snooping profile 1

IGMP-Snooping profile 1
Profile description :
Profile limit       : permit
Profile referred    : e1/1.
start-address        end-address          vlan
224.0.0.1            239.255.255.254      any
Total ip range: 1, mac range: 0

Total profiles: 1, IP&MAC ranges: 1
```

show igmp-snooping record-host

To display the MAC address of the record host, use the **show igmp-snooping record-host** command in the EXEC mode.

show igmp-snooping record-host [*interface-id*]

Syntax Description

record-host	Displays the MAC address of the record host.
interface-id	Displays the MAC address of the record host for the interface.

Command Default

None

Command Modes

User EXEC
Privileged EXEC

Examples

The following eample shows the output of the **show igmp-snooping record-host** command:

```
Device# show igmp-snooping record-host
show host record information
Total Record: 0
```

show igmp-snooping router-dynamic

To display the dynamic route ports, use the **show igmp-snooping router-dynamic** command in the EXEC mode.

show igmp-snooping router-dynamic

Syntax Description

router-dynamic	Displays the dynamic route ports.

Command Default

None

Command Modes

User EXEC
Privileged EXEC

Examples

The following example shows the output from **show igmp-snooping router-dynamic** command on an inteface where IGMP Snooping is enabled:

```
Device# show igmp-snooping router-dynamic
  Port        VID     Age       Type
  e1/3       100     237     { QUERY }
Total Record: 1
```

show igmp-snooping router-static

To display the static route ports on an interface or an a multicast VLAN, use the **show igmp-snooping router-static** command in the EXEC mode.

show igmp-snooping router-static [**interface** {**channel-group** *channel-group-id* | **ethernet** *port*} | **vlan** *vlan-id*]

Syntax Description

router-static	Displays the static router ports.
channel-group-id	Displays the static ports for a LACP channel group. The range is 0-5.
vlan-id	Displays the static ports for Multicast VLANs.

Command Default

None

Command Modes

User EXEC
Privileged EXEC

Examples

The following example shows the output from **show igmp-snooping router-static** command on an inteface where IGMP SNooping is enabled:

```
Device# show igmp-snooping router-static interface  channel-group  1
  Port        VID     Age       Type
Total Record: 0
```

show mld-snooping

To display information about MLD snooping related configuration, use the **show mld-snooping** command in privileged EXEC or global configuration mode.

show mld-snooping

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view information about MLD snooping.

```
Device> enable
Device# configure terminal
Device(config)# show mld-snooping
Enable MLD-Snooping
The max response time is 10 second(s)
The host port timeout is 300 second(s).
Enable MLD-Snooping route-port forward
The Router port timeout is 300 second(s), Currently aging is running
Denied VLAN
Blocked list:
NULL
Allowed list:
NULL
Default group policy is permit
MLD-Snooping Querier : ON
Querier vlan : 101
Max Respond Time 25 sec | Query interval 60 sec
Port Information:
port   groups-limit  fast-leave  mcast-vlan
p0/1   1024          enabled     disabled
p0/2   1024          disabled    disabled
p0/3   1024          disabled    disabled
p0/4   1024          disabled    disabled
p0/5   1024          disabled    disabled
p0/6   1024          disabled    disabled
p0/7   1024          disabled    disabled
p0/8   1024          disabled    disabled
p0/9   1024          disabled    disabled
p0/10  1024          disabled    disabled
p0/11  1024          disabled    disabled
p0/12  1024          disabled    disabled
p0/13  1024          disabled    disabled
p0/14  1024          disabled    disabled
p0/15  1024          disabled    disabled
p0/16  1024          disabled    disabled
e1/1   1024          disabled    disabled
e1/2   1024          disabled    disabled
e1/3   1024          disabled    disabled
e1/4   1024          disabled    disabled
e2/1   1024          disabled    disabled
e2/2   1024          disabled    disabled
```

show mld-snooping router-dynamic

To display the information of dynamic routing port, use the **show mld-snooping router-dynamic** command in privileged EXEC or global configuration mode.

show mld-snooping router-dynamic

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view information about dynamic routing port.

```
Device> enable
Device# configure terminal
Device(config)# show mld-snooping router-dynamic
  Port        VID        Age      Type
  e1/3       101         300    { QUERY }
Total Record: 1
```

show mld-snooping router-static

To display the information of static routing port, use the **show mld-snooping router-static** command in privileged EXEC or global configuration mode.

show mld-snooping router-static

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view information about static routing port.

```
Device> enable
Device# configure terminal
Device(config)# show mld-snooping router-static
  Port        VID        Age      Type
Total Record: 0
```

show multicast mld-snooping

To display multicast information, use the **show multicast mld-snooping** command in privileged EXEC or global configuration mode.

show multicast mld-snooping interface { **ethernet** | **gpon** } *slot-num/port-num*

Syntax Description

slot-num/port-num	The port ID. • *slot-number:* • GPON: The value is 0. • GE Ethernet: The value is 1. • 10GE Ethernet: The value is 2. • *port-number:* • GPON: The range is from 1 to 8. • GE Ethernet: The range is from 1 to 4. • 10GE Ethernet: The range is from 1 to 2

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view information about multicast.

```
Device> enable
Device# configure terminal
Device(config)# show multicast mld-snooping interface gpon 0/1
show mld-snooping multicast table information

MAC Address  :  33:33:00:00:00:0c
IP Address   :  FF02::C
VLAN ID      :  101
Age time     :  274
MLD Port     :  g0/1
MLD Version  :  V1,V2

MAC Address  :  33:33:00:00:00:fb
IP Address   :  FF02::FB
VLAN ID      :  101
Age time     :  283
MLD Port     :  g0/1
MLD Version  :  V1,V2

MAC Address  :  33:33:00:01:00:03
IP Address   :  FF02::1:3
VLAN ID      :  101
Age time     :  299
MLD Port     :  g0/1
MLD Version  :  V2
```

```
MAC Address  :  33:33:ff:00:00:90
IP Address   :  FF02::1:FF00:90
VLAN ID      :  101
Age time     :  265
MLD Port     :  g0/1
MLD Version  :  V1,V2

MAC Address  :  33:33:ff:00:01:01
IP Address   :  FF02::1:FF00:101
VLAN ID      :  101
Age time     :  283
MLD Port     :  g0/1
MLD Version  :  V1,V2

MAC Address  :  33:33:ff:01:04:46
IP Address   :  FF02::1:FF01:446
VLAN ID      :  101
Age time     :  272
MLD Port     :  g0/1
MLD Version  :  V1,V2

MAC Address  :  33:33:ff:0a:7d:ec
IP Address   :  FF02::1:FF0A:7DEC
VLAN ID      :  101
Age time     :  283
MLD Port     :  g0/1
MLD Version  :  V2

MAC Address  :  33:33:ff:35:db:cf
IP Address   :  FF02::1:FF35:DBCF
VLAN ID      :  101
Age time     :  273
MLD Port     :  g0/1
MLD Version  :  V2

MAC Address  :  33:33:ff:3d:30:3b
IP Address   :  FF02::1:FF3D:303B
VLAN ID      :  101
Age time     :  270
MLD Port     :  g0/1
MLD Version  :  V1,V2

MAC Address  :  33:33:ff:53:25:fe
IP Address   :  FF02::1:FF53:25FE
VLAN ID      :  101
Age time     :  283
MLD Port     :  g0/1
MLD Version  :  V1,V2

MAC Address  :  33:33:ff:87:2c:93
IP Address   :  FF02::1:FF87:2C93
VLAN ID      :  101
Age time     :  276
MLD Port     :  g0/1
MLD Version  :  V1,V2

MAC Address  :  33:33:ff:8d:03:30
IP Address   :  FF02::1:FF8D:330
VLAN ID      :  101
Age time     :  279
MLD Port     :  g0/1
MLD Version  :  V1,V2
```

```
MAC Address  :  33:33:ff:a2:7b:3e
IP Address   :  FF02::1:FFA2:7B3E
VLAN ID      :  101
Age time     :  270
MLD Port     :  g0/1
MLD Version  :  V1,V2

MAC Address  :  33:33:ff:ba:22:cb
IP Address   :  FF02::1:FFBA:22CB
VLAN ID      :  101
Age time     :  283
MLD Port     :  g0/1
MLD Version  :  V1,V2

MAC Address  :  33:33:ff:da:4e:79
IP Address   :  FF02::1:FFDA:4E79
VLAN ID      :  101
Age time     :  270
MLD Port     :  g0/1
MLD Version  :  V1,V2

MAC Address  :  33:33:ff:e5:01:41
IP Address   :  FF02::1:FFE5:141
VLAN ID      :  101
Age time     :  283
MLD Port     :  g0/1
MLD Version  :  V1,V2

Total Record: 16
```

show multicast igmp-snooping

To display igmp-snooping multicast table information, use the **show multicast igmp-snooping** command in the EXEC mode.

show multicast igmp-snooping { **interface***interface-id* | **ip-address** *ip-address* }

Syntax Description

interface-id	Displays the IGMP Snooping multicast table for the interface.
ip-address	Displays the IGMP Snooping multicast table for the IP address.

Command Default

None

Command Modes

User EXEC
Privileged EXEC

Examples

The following example displays the output of the **show multicast igmp snooping** command for an interface:

```
Device# show multicast igmp-snooping interface ethernet 1/1
show igmp-snooping multicast table information Total Record: 0
```

show ont multicast

To display information about the multicast learning table on an ONT, use the **show ont multicast** command in privileged EXEC or global configuration mode.

show ont multicast *slot-num/pon-num/ont-num* [**port** *port-id*]

Syntax Description

slot-num/pon-num/ont-num	The ONT ID. • *slot-num*: The slot number. The value is 0. • *pon-num*: The PON number. The range is fro • *ont-num*: The ONT number. The range is fro
port-id	The ONT Ethernet port ID. The range is from 1 to 24.

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the information about the multicast learning table on an ONT.

```
Device> enable
Device# configure terminal
Device(config)# show ont multicast 0/1/1
```

show running-config mld_snooping

To display the running MLD Snooping configuration, use the **show running-config mld_snooping** command in the EXEC mode.

show running-config mld_snooping

Syntax Description		
	mld_snooping	Displays the running MLD snooping configuration.

Command Default

None.

Command Modes

User EXEC
Priveleged EXEC

The following example shows a sample output of the show running-config mld_snooping command.

```
Device#show running-config mld_snooping

![MLD_SNOOPING]
mld-snooping
mld-snooping route-port forward
mld-snooping query-max-respond 25
mld-snooping querier
mld-snooping querier-vlan 101
interface gpon 0/1
mld-snooping fast-leave
mld-snooping record-host
mld-snooping multicast vlan 1
exit
```

PART IX

System Management

System Management

alarm all-packets

To enable alarms on all ports, use the **alarm all-packets** command in global configuration mode.

To enable alarms on a specific port, use the **alarm all-packets** command in interface configuration mode.

alarm all-packets

no alarm all-packets

Command Modes

Global configuration (config)

Interface configuration (config-if)

Examples

The following example shows how to enable alarms on all ports of the device:

```
Device> enable
Device# configure terminal
Device(config)# alarm all-packets
Enable port alarm successfully.
```

alarm all-packets threshold

To configure the port threshold information for alarms, use the **alarm all-packets threshold** command in interface configuration mode.

alarm all-packets threshold {**normal** *normal-value* | **exceed** *exceed-value*}

Syntax Description

normal *normal-value*	Sets the minimum port bandwidth utilization threshold for the port.
exceed *exceed-value*	Sets the maximum port bandwidth utilization threshold for the port.

Command Modes

Interface configuration mode (config-if)

Examples

The following example shows how to set the port thresholds using the **alarm all-packets threshold** command:

```
Device> enable
Device# configure terminal
Device(config)# interface gpon 0/1
Device(config-if-gpon-0/1)# alarm all-packets threshold exceed 34 normal 4
```

alarm cpu

To enable CPU alarms, use the **alarm cpu** command in global configuration mode.

alarm cpu
no alarm cpu

Command Modes

Global configuration mode (config)

Examples

The following example shows how to enable CPU alarms:

```
Device> enable
Device# configure terminal
Device(config)# alarm cpu
```

alarm cpu threshold

To configure the threshold information for CPU alarms, use the **alarm cpu threshold** command in global configuration mode.

alarm cpu threshold {**busy** *busy-value* | **unbusy** *unbusy-value*}

Syntax Description

busy *busy-value*	Sets the minimum CPU utilization threshold.
unbusy *unbusy-value*	Sets the maximum CPU utilization threshold.

Command Modes

Global configuration mode (config)

Examples

The following example shows how to set the CPU thresholds using the **alarm cpu threshold** command:

```
Device> enable
Device# configure terminal
Device(config)# alarm cpu threshold busy 63 unbusy 20
```

buildrun mode

To configure the file execution mode, use the **buildrun mode** command in privileged EXEC mode.

buildrun mode {**continue** | **stop**}

Syntax Description

continue	Sets the execution mode to non-interruptible.
stop	Sets the execution mode to interruptible.

Command Modes

Privileged EXEC (#)

Examples

The following is an example of the **buildrun mode stop** command:

```
Device> enable
Device# buildrun mode stop
```

clear startup-config

To clear the startup configuration, use the **clear startup-config** command in privileged EXEC mode.

clear startup-config

Command Modes

Privileged EXEC (#)

Examples

The following is an example of the **clear startup-config**command:

```
Device> enable
Device# clear startup-config
```

clock summer-time

To set the clock daylight savings time, use the **clock summer-time** command in global configuration mode.

clock summer-time { **dayly** | **weekly** } *start-time*

Syntax Description

start-time	Specifies the start time for daylight savings. The daylight savings time format must be entered in hour, minutes and, seconds (HH:MM:SS).

Command Modes

Global configuration mode (config)

Examples

The following example shows how to configure the daylight savings using the **clock summer-time** command:

```
Device> enable
Device# configure terminal
Device(config)# clock summer-time dayly 00:00:00 2021/03/12 00:00:00 2021/11/05
```

clock timezone

To configure the system time zone, use the **clock timezone** command in global configuration mode.

clock timezone *timezone-name hours-offset minutes-offset*
no clock timezone

Syntax Description

timezone-name	Specifies the timezone to the SNTP client.
hours-offset minutes-offset	Specifies the hours and minutes offset from the timezone to the SNTP client.

Command Modes

Global configuration mode (config)

Examples

The following example shows how to configure a timezone on the SNTP client using the **clock timezone** command:

```
Device> enable
Device# configure terminal
Device(config)# clock timezone ch 3 43
```

copy running-config startup-config

To copy the current configuration to the flash config file, use the **copy running-config startup-config** command in privileged EXEC mode.

copy running-config startup-config

Command Modes

Privileged EXEC (#)

Examples

The following is an example of the **copy running-config startup-config** command:

```
Device> enable
Device# copy running-config startup-config
Startup config in flash will be updated, are you sure(y/n)? [n]
```

copy startup-config running-config

To copy the startup configuration from the flash config file to the current configuration, use the **copy startup-config running-config** command in privileged EXEC mode.

copy startup-config running-config

Command Modes

Privileged EXEC (#)

Examples

The following is an example of the **copy startup-config running-config** command:

```
Device> enable
Device# copy startup-config running-config
Running config will be updated, are you sure(y/n)? [n]
```

load ftp

To download a file with the FTP server, use the **load ftp** command in privileged EXEC mode.

load {**application** | **configuration** | **edfa** | **epld** | **keyfile** {**private** | **public**} | **ont-image** | **whole-bootrom**}**ftp** {**inet** | **inet6**}*ftp-server-ip-address file-name ftp-username ftp-password*

Syntax Description

application	Specifies the host file.
configuration	Specifies the configuration file.
edfa	Specifies the EDFA file.
epld	Specifies the EPLD file.
keyfile	Specifies the SSH keyfile.
private	Specifies the SSH private keyfile.
public	Specifies the SSH public keyfile.
ont-image	Specifies the ONT image file.
whole-bootrom	Specifies the whole bootrom file.
inet	Specifies IPv4 address family.
inet6	Specifies IPv6 address family.
ftp-server-ip-address	Specifies the IP address of the FTP server.
file-name	Specifies the name of the file to be uploaded.
ftp-username	Specifies the user name of the FTP server.
ftp-password	Specifies the password of the FTP server.

Command Modes

Privileged EXEC (#)

Examples

The following example shows how to download a whole bootrom file with an FTP server using the **load ftp** command:

```
Device> enable
Device# load whole-bootrom tftp inet 10.23.13.1 bootrom1.bin
```

load tftp

To download a file with the TFTP server, use the **load tftp** command in privileged EXEC mode.

load {**application** | **configuration** | **edfa** | **epld** | **keyfile** {**private** | **public**} | **ont-image** | **whole-bootrom**}**tftp** {**inet** | **inet6**}*tftp-server-ip-address file-name*

Syntax Description

application	Specifies the host file.
configuration	Specifies the configuration file.
edfa	Specifies the EDFA file.
epld	Specifies the EPLD file.
keyfile	Specifies the SSH keyfile.
private	Specifies the SSH private keyfile.
public	Specifies the SSH public keyfile.
ont-image	Specifies the ONT image file.
whole-bootrom	Specifies the whole bootrom file.
inet	Specifies IPv4 address family.
inet6	Specifies IPv6 address family.
tftp-server-ip-address	Specifies the IP address of the TFTP server.
file-name	Specifies the name of the file to be uploaded.

Command Modes

Privileged EXEC (#)

Examples

The following example shows how to download a whole bootrom file with a TFTP server using the **load tftp** command:

```
Device> enable
Device# load whole-bootrom tftp inet6 10:23::11:1 bootrom1.bin
```

load xmodem

To download a file with the XMODEM, use the **load ftp** command in privileged EXEC mode.

load {**application** | **configuration** | **whole-bootrom**}**xmodem**

Syntax Description

application	Specifies the host file.
configuration	Specifies the configuration file.
whole-bootrom	Specifies the whole bootrom file.

Command Modes

Privileged EXEC (#)

Examples

The following example shows how to download a whole bootrom file with an XMODEM using the **load xmodem** command:

```
Device> enable
Device# load whole-bootrom xmodem
```

local fec

To enable the ONT uplink FEC, use the **local fec** command in line profile configuration mode. To disable the ONT uplink FEC, use the **no local fec** command.

local fec

no local fec

Command Modes

Line profile configuration (deploy-profile-line)

Examples

This example shows how to enable the ONT uplink FEC

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(config-profile-line)# aim 5
Device(config-profile-line-5)# local fec
```

ntp access

To configure access control for Network Time Protocol (NTP) services, use the **ntp access** command in global configuration mode. To disable NTP settings, use the **no access** form of the command.

ntp access *ip-address* { **permit** | **deny** }

no ntp access *ip-address* { **permit** | **deny** }

Syntax Description

access *ip-address*	Specifies the control access for an IPv4 or IPv6 access list to the NTP services.
permit	Permts the NTP services.
deny	Denies the NTP services

Command Modes

Global configuration (config)

Examples

The following example shows how to enable NTP authentication using the **ntp access** command:

```
Device> enable
Device# configure terminal
Device(config)# ntp access 192.168.0.10 255.255.255.0 permit
```

ntp authentication

To enable NTP authentication and configure NTP settings, use the **ntp authenticatiom** command in global configuration mode. To disable NTP settings, use the **no** form of the command.

ntp authentication authentication-keyid *key_id* **md5** *key_string*

no ntp authentication authentication-keyid *key_id* **md5** *key_string*

Syntax Description

authentication	Enables NTP authentication.
authentication-keyid *key_id* **md5** *key_string*	Specifies an authentication key for a trusted NTP source. • *key_id*: The authentication key. The range is from 1 to 65535. • **md5**: Message Digest 5 (MD5) algorithm authentication support • *key_string*: Key value. The maximum length is 32 characters.

Command Modes

Global configuration (config)

Examples

The following example shows how to enable NTP authentication using the **ntp authentication** command:

```
Device> enable
Device# configure terminal
Device(config)# ntp authentication
```

ntp broadcast

To configure NTP broadcast mode, use the **ntp broadcast** command in interface configuration mode. To disable NTP settings, use the **no** form of the command.

ntp broadcast { **server authentication-keyid** *key_id* | **client** }

no ntp broadcast { **server authentication-keyid** *key_id* | **client** }

Syntax Description

authentication-keyid *key_id*	Specifies an authentication key for a trusted NTP source. *key_id*: The authentication key. The range is from 1 to 65535.

Command Modes

Interface configuration (config-if)

Examples

The following example shows how to configure the NTP broadcast mode using **ntp broadcast** command:

```
Device> enable
Device# configure terminal
Device(config)# interface vlan-interface 1
Device(config-if-vlaninterface-1)# ntp broadcast server
```

ntp disable

To disable NTP incoming packets, use the **ntp disable** command in interface configuration mode. To disable NTP settings, use the **no** form of the command.

ntp disable

no ntp disable

Command Modes

Interface configuration (config-if)

Examples

The following example shows how to disable NTP incoming packets using the **ntp disable** command:

```
Device> enable
Device# configure terminal
Device(config)# interface vlan-interface 1
Device(config-if-vlaninterface-1)# ntp disable
```

ntp max-dynamic-sessions

To configure maximum number of dynamic NTP sessions, use the **ntpmax-dynamic-sessions** command in global configuration mode. To disable NTP settings, use the **no** form of the command.

ntp max-dynamic-sessions *value*

no ntp max-dynamic-sessions *value*

Syntax Description

max-dynamic-sessions *value*	Specifies the maximum number of dynamic sessions. *value*: The range is from 11 to 100.

Command Modes

Interface configuration (config-if)

Examples

The following example shows how to configure maximum number of dynamic NTP sessions using the **ntp authentication** command:

```
Device> enable
Device# configure terminal
Device(config)# ntp max-dynamic-sessions 10
```

ntp multicast

To configure NTP multicast mode, use the **ntp multicast** command in global configuration mode. To disable NTP settings, use the **no** form of the command.

ntp multicast { **server authentication-keyid** *key_id* | **client** }

no ntp multicast { **server authentication-keyid** *key_id* | **client** }

Syntax Description

authentication-keyid *key_id*	Specifies an authentication key for a trusted NTP source. *key_id*: The authentication key. The range is from 1 to 65535.

Command Modes

Interface configuration (config-if)

Examples

The following example shows how to configure the NTP multicast mode using **ntp multicast** command:

```
Device> enable
Device# configure terminal
Device(config)# interface vlan-interface 1
Device(config-if-vlaninterface-1)# ntp multicast server
```

ntp unicast peer

To configure synchronization to an NTP-configured peer device, use the **ntp unicast peer** command in global configuration mode. To disable NTP settings, use the **no** form of the command.

ntp unicast peer *ip-address* [**authentication-keyid** *key_id*]

no ntp unicast peer *ip-address* [**authentication-keyid** *key_id*]

Syntax Description

peer *ip-address*	Specifies the system clock to synchronize a peer or to be synchronized by a peer *ip-address*: IPv4 or IPv6 address of the peer device.

Command Modes

Global configuration (config)

Examples

The following example shows how to configure synchronization to an NTP-configured peer device using the **ntp unicast peer** command:

```
Device> enable
Device# configure terminal
Device(config)# ntp unicast peer 192.168.0.10
```

ntp unicast server

To configure client mode, use the **ntp unicast server** command in global configuration mode. To disable NTP settings, use the **no** form of the command.

ntp unicast server *ip-address* [**authentication-keyid** *key_id*]

no ntp unicast server *ip-address* [**authentication-keyid** *key_id*]

Syntax Description

server*ip-address*	Specifies the system clock to be synchronized by a time server. *ip-address*: IPv4 or IPv6 address of the time server.

Command Modes

Global configuration (config)

Examples

The following example shows how to configure client mode using the **ntp unicast server** command:

```
Device> enable
Device# configure terminal
Device(config)# ntp unicast server  192.168.0.11
```

show alarm all-packets

To display the port alarm information, use the **show alarm all-packets** command in global configuration mode or interface configuration mode.

show alarm all-packets [**interface** *port-number*]

Syntax Description

interface *port-number*	Specifies the interface.

Command Modes

Global configuration mode (config)

Interface configuration mode (config-if)

Examples

The following is a sample output of the **show alarm all-packets** command:

show alarm cpu

To display the CPU alarm information, use the **show alarm all-packets** command in global configuration mode.

show alarm cpu

Command Modes

Global configuration mode (config)

Examples

The following is a sample output of the **show alarm cpu** command:

```
Device(config)# show alarm cpu
CPU status alarm : enable
CPU busy threshold(%) : 90
CPU unbusy threshold(%) : 85
CPU status : unbusy
```

show clock

To display the system clock, use the **show clock** command in global configuration mode.

show clock

Command Modes

Global configuration mode (config)

Examples

The following is a sample output of the **show clock** command:

```
Device> enable
Device# configure terminal
Device(config)# show clock
Mon 2020/4/30 04:25:07 CCT 08:00
```

show ntp access

To display the NTP access configuration, use the **show ntp access** command in global configuration mode.

show ntp access

Command Modes

Global configuration mode (config)

Examples

The following is a sample output of the **show ntp access** command:

```
Device> enable
Device# configure terminal
Device(config)# show ntp access
```

show ntp authentication

To display NTP authentication configuration, use the **show ntp authentication** command in global configuration mode.

show ntp authentication

Command Modes

Global configuration mode (config)

Examples

The following is a sample output of the **show ntp authentication** command:

```
Device> enable
Device# configure terminal
Device(config)# show ntp authentication
```

show ntp broadcast server

To display the NTP broadcast server configuration, use the **show ntp broadcast server** command in global configuration mode.

show ntp broadcast server

Command Modes

Global configuration mode (config)

Examples

The following is a sample output of the **show ntp broadcast server** command:

```
Device> enable
Device# configure terminal
Device(config)# show ntp broadcast server
```

show ntp disable

To disable NTP configuration, use the **show ntp disable** command in global configuration mode.

show ntp disable

Command Modes

Global configuration mode (config)

Examples

The following is a sample output of the **show ntp disable** command:

```
Device> enable
Device# configure terminal
Device(config)# show ntp disable
```

show ntp max-dynamic-sessions

To display the maximum number of dynamic sessions, use the **show ntp max-dynamic-sessions** command in global configuration mode.

show ntp max-dynamic-sessions

Command Modes

Global configuration mode (config)

Examples

The following is a sample output of the **show ntp max-dynamic-sessions** command:

```
Device> enable
Device# configure terminal
Device(config)# show ntp max-dynamic-sessions
```

show ntp multicast server

To display the NTP multicast server configuration, use the **show ntp multicast server** command in global configuration mode.

show ntp multicast server

Command Modes

Global configuration mode (config)

Examples

The following is a sample output of the **show ntp multicast server** command:

```
Device> enable
Device# configure terminal
Device(config)# show ntp multicast server
```

show ntp sessions

To display the NTP session details, use the **show ntp sessions** command in global configuration mode.

show ntp sessions

Command Modes

Global configuration mode (config)

Examples

The following is a sample output of the **show ntp sessions** command:

```
Device> enable
Device# configure terminal
Device(config)# show ntp sessions
```

show ntp status

To display the NTP status configuration, use the **show ntp status** command in global configuration mode.

show ntp status

Command Modes

Global configuration mode (config)

Examples

The following is a sample output of the **show ntp status** command:

```
Device> enable
Device# configure terminal
Device(config)# show ntp status
```

show ntp unicast peer

To display the NTP unicast peer configuration, use the **show ntp unicast peer** command in global configuration mode.

show ntp unicast peer

Command Modes

Global configuration mode (config)

Examples

The following is a sample output of the **show ntp unicast peer** command:

```
Device> enable
Device# configure terminal
Device(config)# show ntp unicast peer
```

show ntp unicast server

To display the NTP unicast server configuration, use the **show ntp unicast server** command in global configuration mode.

show ntp unicast server

Command Modes

Global configuration mode (config)

Examples

The following is a sample output of the **show ntp unicast server** command:

```
Device> enable
Device# configure terminal
Device(config)# show ntp unicast server
```

show running-config

To display the current system configuration, use the **show running-config** command in the privileged EXEC mode or global configuratoin mode.

show running-config {*module* | **interface** {**ethernet** *port-id* | **gpon** *port-id* | **loopback-interface** *loopback-interface-number* | **vlan-interface** *vlan-id*}}**perlines** *lines-per-page*

Syntax Description

module	Specifies a module.
interface	Specifies an interface.
ethernet *port-id*	Displays the ethernet port configuration.
gpon *port-id*	Displays the GPON port configuration.
loopback-interface *loopback-interface-number*	Displays the loopback interface configuration.
vlan-interface *vlan-id*	Displays the VLAN configuration.
perlines *lines-per-page*	Specifies the number of lines displayed per page.

Command Modes

Privileged EXEC (#)

Global configuration mode (config)

Examples

The following is a sample output from the **show running-config interface vlan-interface** command:

```
Device> enable
Device# show running-config interface vlan-interface

Building configuration...
![vlan-interface 1]
ip address range 192.0.2.254 192.0.2.255
description interface1
![vlan-interface 100]
ip address 10.75.171.17 255.255.255.0
end
```

show sntp client

To display SNTP client configurations, use the **show sntp client** command in global configuration mode.

show sntp client

Command Modes

Global configuration mode (config)

Examples

The following is a sample output of the **show sntp client** command:

```
Device> enable
Device# configure terminal
Device(config)# show sntp client
Clock state : synchronized         Current mode : anycast
Use server : 192.168.1.99          State : idle
Server state : synchronized        Server stratum : 1
Retrans-times: 3                   Retrans-interval: 30s
Authenticate : enable              Authentication-key: 1
Poll interval : 1000s
Last synchronized time: THU NOV 26 09:22:25 2015
```

show startup-config

To display the startup configuration, use the **show startup-config** command in the privileged EXEC mode or global configuratoin mode.

show startup-config {*module* | **interface** {**ethernet** *port-id* | **gpon** *port-id* | **loopback-interface** *loopback-interface-number* | **vlan-interface** *vlan-id*}}**perlines** *lines-per-page*

Syntax Description

module	Specifies a module.
interface	Specifies an interface.
ethernet *port-id*	Displays the ethernet port configuration.
gpon *port-id*	Displays the GPON port configuration.
loopback-interface *loopback-interface-number*	Displays the loopback interface configuration.
vlan-interface *vlan-id*	Displays the VLAN configuration.
perlines *lines-per-page*	Specifies the number of lines displayed per page.

Command Modes

Privileged EXEC (#)

Global configuration mode (config)

Examples

The following is a sample output from the **show startup-config interface ethernet** command:

```
Device> enable
Device# show startup-config interface ethernet

Building configuration...
![ethernet 1/1]
channel-group 2 mode on
lacp port-priority 8
description text
switchport hybrid untagged vlan 2-125
igmp-snooping record-host
ip-source-guard ip-mac-vlan
![ethernet 1/2]
switchport hybrid tagged vlan 35,335
switchport hybrid untagged vlan 2-34,36-125,2501-2502
![ethernet 1/3]
switchport default vlan 100
switchport hybrid untagged vlan 2-125
![ethernet 1/4]
priority 2
![ethernet 2/1]
switchport hybrid untagged vlan 2-125
![ethernet 2/2]
switchport hybrid untagged vlan 2-125
end
```

sntp client

To enable SNTP client, use the **sntp client** command in global configuration mode.

sntp client

no sntp client

Command Modes

Global configuration mode (config)

Examples

The following example shows how to enable SNTP client:

```
Device> enable
Device# configure terminal
Device(config)# sntp client
```

sntp client authenticate

To enable authentication of time sources, use the **sntp client authenticate** command in global configuration mode.

sntp client authenticate
no sntp client authenticate

Command Modes

Global configuration mode (config)

Examples

The following example shows how to enable SNTP client authentication using the **sntp client authenticate** command:

```
Device> enable
Device# configure terminal
Device(config)# sntp client authenticate
```

sntp client authentication-key

To configure the password for authentication for trusted time sources, use the **sntp client authentication-key** command in global configuration mode.

sntp client authentication-key *key-number* **md5** *md5-key*
no sntp client authentication-key *key-number*

Syntax Description

key-number	Specifies the authentication key for the SNTP client.
md5 *md5-key*	Specifies the MD5 authentication key for the SNTP client.

Command Modes

Global configuration mode (config)

Examples

The following example shows how to configure SNTP client authentication using the **sntp client authentication-key** command:

```
Device> enable
Device# configure terminal
Device(config)# sntp client authentication-key 3 md5 5
```

sntp client broadcastdelay

To configure the broadcast propagation delay for an SNTP client, use the **sntp client broadcastdelay** command in global configuration mode.

sntp client broadcastdelay *delay-time*

Syntax Description

delay-time	Specifies the round-trip broadcast delay for the SNTP client in milliseconds.

Command Modes

Global configuration mode (config)

Examples

The following example show how to configure the delay time for the SNTP client using the **sntp client broadcastdelay** command:

```
Device> enable
Device# configure terminal
Device(config)# sntp client broadcastdelay 15
```

sntp client mode

To configure the mode of function of the SNTP client, use the **sntp client mode** command in global configuration mode.

sntp client mode {**anycast** {[**key** *key-id*]} | **broadcast** | **multicast** | **unicast**}

Syntax Description

anycast	Sets the SNTP client to work in anycast mode.
key *key-id*	Specifies the authentication key for anycast mode.
broadcast	Sets the SNTP client to work in broadcast mode.
multicast	Sets the SNTP client to work in multicast mode.
unicast	Sets the SNTP client to work in unicast mode.

Command Modes

Global configuration mode (config)

Examples

The following example show how to configure the SNTP client to unicast mode using the **sntp client mode** command:

```
Device> enable
Device# configure terminal
Device(config)# sntp client mode unicast
```

sntp client poll-interval

To configure the polling interval for an SNTP client, use the **sntp client poll-interval** command in global configuration mode.

sntp client poll-interval *poll-interval-time*

Syntax Description

poll-interval-time	Specifies the polling interval for the SNTP client in seconds.

Command Modes

Global configuration mode (config)

Examples

The following example show how to configure the polling interval for the SNTP client using the **sntp client poll-interval** command:

```
Device> enable
Device# configure terminal
Device(config)# sntp client poll-interval 800
```

sntp client retransmit-interval

To configure the timeout retransmission interval for an SNTP client, use the **sntp client retransmit-interval** command in global configuration mode.

sntp client retransmit-interval *retransmit-interval-time*

Syntax Description

retransmit-interval-time	Specifies the timeout retransmission interval for the SNTP client in seconds.

Command Modes

Global configuration mode (config)

Usage Guidelines

The configured timeout retransmission mechanism takes effect only when the SNTP client works in the unicast or anycast mode.

Examples

The following example show how to configure the retransmission interval for the SNTP client using the **sntp client retransmit-interval** command:

```
Device> enable
Device# configure terminal
Device(config)# sntp client retransmit-interval 8
```

sntp client retransmit

To configure the number of timeout retransmission attempts for an SNTP client, use the **sntp client retransmit** command in global configuration mode.

sntp client retransmit *number*

Syntax Description

number	Specifies the number of timeout retransmission attempts for the SNTP client.

Command Modes

Global configuration mode (config)

Usage Guidelines

The configured timeout retransmission mechanism takes effect only when the SNTP client works in the unicast or anycast mode.

Examples

The following example show how to configure the number of retransmission attempts for the SNTP client using the **sntp client retransmit-interval** command:

```
Device> enable
Device# configure terminal
Device(config)# sntp client retransmit 5
```

sntp client valid-server

To configure a legal server list for the SNTP client, use the **sntp client valid-server** command in global configuration mode.

sntp client valid-server *ip-address wildcard-ip-address*
no sntp client valid-server {**all** | *ip-address wildcard-ip-address*}

Syntax Description

ip-address	Specifies the IP address of the valid SNTP server.
wildcard-ip-address	Specifies the IP address of the wildcard SNTP server.

Command Modes

Global configuration mode (config)

Examples

The following example shows how to configure the valid SNTP servers for an SNTP client using the **sntp client valid-server** command:

```
Device> enable
Device# configure terminal
Device(config)# sntp client valid-server 10.23.23.1 23.1.1.4
```

sntp server

To set SNTP server configurations, use the **sntp server** command in global configuration mode.

sntp server {*ip-address* | **backup** *ip-address* | **key** *key-number*}

Syntax Description

ip-address	Specifies the IP address of the SNTP server.
backup *ip-address*	Specifies the IP address of the SNTP backup server.
key *key-number*	Specifies the authentication key for the SNTP server.

Command Modes

Global configuration mode (config)

Examples

The following example shows how to configure the SNTP server using the **sntp server** command:

```
Device> enable
Device# configure terminal
Device(config)# sntp server 12.2.2.1
```

sntp trusted-key

To configure a trusted password for multicast and broadcast modes, use the **sntp trusted-key** command in global configuration mode.

sntp trusted-key *key-number*
no sntp trusted-key *key-number*

Syntax Description

key-number	Specifies the trusted key for the SNTP client.

Command Modes

Global configuration mode (config)

Examples

The following example shows how to configure SNTP client trusted key authentication using the **sntp trusted-key** command:

```
Device> enable
Device# configure terminal
Device(config)# sntp trusted-key 243586
```

upload automatically configuration ftp

To automatically upload a configuration file at regular intervals with the FTP server, use the **upload automatically configuration ftp** command in privileged EXEC mode.

upload automatically configuration ftp {**inet** | **inet6**}*ftp-server-ip-address file-name ftp-username ftp-password***per hours** *hours* **minutes** *minutes*

Syntax Description

inet	Specifies IPv4 address family.
inet6	Specifies IPv6 address family.
ftp-server-ip-address	Specifies the IP address of the FTP server.
file-name	Specifies the name of the file to be uploaded.
ftp-username	Specifies the user name of the FTP server.
ftp-password	Specifies the password of the FTP server.
per hours *hours* **minutes** *minutes*	Specifies the time interval in hours and minutes after which the configuration file is to be automatically uploaded.

Command Modes

Privileged EXEC (#)

Examples

The following example shows how to upload a configuration file using the **upload automatically configuration tftp** command:

```
Device> enable
Device# upload automatically configuration ftp inet 10.23.13.1 config3.txt per hours 12
minutes 10
```

upload automatically configuration tftp

To automatically upload a configuration file at regular intervals with the TFTP server, use the **upload automatically configuration tftp** command in privileged EXEC mode.

upload automatically configuration tftp {**inet** | **inet6**}*tftp-server-ip-address file-name* **per hours** *hours* **minutes** *minutes*

Syntax Description

inet	Specifies IPv4 address family.
inet6	Specifies IPv6 address family.
tftp-server-ip-address	Specifies the IP address of the TFTP server.
file-name	Specifies the name of the file to be uploaded.
per hours *hours* **minutes** *minutes*	Specifies the time interval in hours and minutes after which the configuration file is to be automatically uploaded.

Command Modes

Privileged EXEC (#)

Examples

The following example shows how to upload a configuration file using the **upload automatically configuration tftp** command:

```
Device> enable
Device# upload automatically configuration tftp inet 10.23.13.1 config2.txt per hours 20
minutes 30
```

upload ftp

To upload a file with the FTP server, use the **upload ftp** command in privileged EXEC mode.

upload {**application** | **configuration** | **keyfile** {**private** | **public**} | **logging**}**ftp** {**inet** | **inet6**}*ftp-server-ip-address file-name ftp-username ftp-password*

Syntax Description

application	Specifies the host file.
configuration	Specifies the configuration file.
keyfile	Specifies the SSH keyfile.
private	Specifies the SSH private keyfile.
public	Specifies the SSH public keyfile.
logging	Specifies the log file.
inet	Specifies IPv4 address family.
inet6	Specifies IPv6 address family.
ftp-server-ip-address	Specifies the IP address of the FTP server.
file-name	Specifies the name of the file to be uploaded.
ftp-username	Specifies the user name of the FTP server.
ftp-password	Specifies the password of the FTP server.

Command Modes

Privileged EXEC (#)

Examples

The following example shows how to upload a host file with an FTP server using the **upload ftp** command:

```
Device> enable
Device# upload application ftp 192.168.1.99 host.arj rr 142
```

upload tftp

To upload a file with the TFTP server, use the **upload tftp** command in privileged EXEC mode.

upload {**application** | **configuration** | **keyfile** {**private** | **public**} | **logging**}**tftp** {**inet** | **inet6**}*tftp-server-ip-address file-name*

Syntax Description

application	Specifies the host file.
configuration	Specifies the configuration file.
keyfile	Specifies the SSH keyfile.
private	Specifies the SSH private keyfile.
public	Specifies the SSH public keyfile.
logging	Specifies the log file.
inet	Specifies IPv4 address family.
inet6	Specifies IPv6 address family.
tftp-server-ip-address	Specifies the IP address of the TFTP server.
file-name	Specifies the name of the file to be uploaded.

Command Modes

Privileged EXEC (#)

Examples

The following example shows how to upload a configuration file with a TFTP server using the **upload tftp** command:

```
Device> enable
Device# upload application tftp 192.168.1.99 text.txt
```

PART X

ONT Device Configuration

ONT Device Configuration

alarm profile refer

To refer an alarm profile to a line profile, use the **alarm profile refer** command in line profile configuration mode.

alarm profile refer {*index_num* | **name** *name*}

Syntax Description

index_num	The alarm profile index number. The range is from 1 to 127.
name	The alarm profile name. The unit is string. The string length is from 1 to 1

Command Modes

Line profile configuration (deploy-profile-line)

Examples

This example shows how to refer an alarm profile to a line profile

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 5
Device(deploy-profile-line-5)# alarm profile refer 1
```

clear ont-logging buffer

To clear the ont logging buffer, use the **clear ont-logging buffer** command in global configuration mode.

clear ont-logging buffer {*ont_id_list* | **all**}

Syntax Description

ont_id_list	The list of ONT IDs.
all	All ONTs.

Command Modes

Global configuration (config)

Examples

This example shows how to clear the ONT log buffering

```
Device> enable
Device# configure terminal
Device(config)# clear ont-logging buffer all
```

local bandwidth egress

To configure the ONT bandwidth egress, use the **local bandwidth egress port** *port_id* **cir** *cir* **cbs** *cbs* **pir** *pir* **pbs** *pbs* command in line profile configuration mode. To disable the ONT bandwidth egress, use the **no local bandwidth egress port** *port_id* command.

local bandwidth egress port *port_id* **cir** *cir* **cbs** *cbs* **pir** *pir* **pbs** *pbs*

no local bandwidth egress port *port_id*

Syntax Description

port_id	The ONT Ethernet port ID. The range is from 1 to 24.
cir *cir*	The committed information rate in kbps. The value range is from
cbs *cbs*	The committed burst size in KB. The value range is from 2 to 320
pir *pir*	The peak information rate in kbps. The value range is from 64 to is greater than or equal to CIR.
pbs *pbs*	The peak burst size in KB. The value range is from 2 to 32000.

Command Modes

Line profile configuration (deploy-profile-line)

Examples

This example shows how to configure the ONT bandwidth egress.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 5
Device(deploy-profile-line-5)# local bandwidth egress port 3 cir 200 cbs 70 pir 1024 pbs
90
```

local loop-detect

To enable local loop-detect, use the **local loop-detect** command in line profile configuration mode. To disable local loop-detect, use the **no local loop-detect** command.

local loop-detect

no local loop-detect

Command Modes

Line profile configuration (deploy-profile-line)

Examples

This example shows how to enable local loop-detect

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 5
Device(deploy-profile-line-5)# local loop-detect
```

local mac-address-table

To configure the ONT maximum MAC count, use the **local mac-address-table** command in line profile configuration mode. To disable the ONT maximum MAC count, use the **no local mac-address-table** command.

local mac-address-table max-mac-count *max_mac_count* [**port** *port_id*]

no local mac-address-table

Syntax Description

max_mac_count	The maximum MAC address learning c The range is from 1 to 255.
port_id	The ONT Ethernet port ID. The range i

Command Modes

Line profile configuration (deploy-profile-line)

Examples

This example shows how to configure the ONT maximum MAC count.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 5
Device(deploy-profile-line-5)# local mac-address-table max-mac-count 12
```

local neg-mode

To configure the local Ethernet speed and duplex, use the **local neg-mode speed** *speed* **duplex** *duplex_mode* **port** *port_id* command in unique profile configuration mode.

local neg-mode speed *speed* **duplex** *duplex_mode* **port** *port_id*

Syntax Description

speed	The ONT Ethernet port rate mode. The options are • 10M • 100M • 1000M • Auto-negotiation
duplex_mode	The ONT Ethernet port duplex mode. The options are • Full-duplex • Half-duplex • Auto-negotiation
port_id	The ONT Ethernet port ID. The range is fro

Command Modes

Unique profile configuration (deploy-profile-unique)

Examples

This example shows how to configure the local Ethernet speed and duplex

```
Device> enable
Device# configure terminal
Device(config)# deploy profile unique
Device(deploy-profile-unique)# aim 0/1/1
Device(deploy-profile-unique-0/1/1)# local neg-mode speed 10 duplex half port 3
```

local ranging-balance

To configure ONT range compensation, use the **local ranging-balance** command in unique profile configuration mode. To disable the ONT range compensation, use the **no local ranging-balance** command.

local ranging-balance {**decrease** | **increase**}*balance_length*

no local ranging-balance

Syntax Description

decrease	Decreases the range compensation.
increase	Increases the range compensation.
balance_length	The ONT ranging compensation value The unit is meters. The range is from 1 to 100

Command Modes

Unique profile configuration (deploy-profile-unique)

Examples

This example shows how to increase ONT range compensation

```
Device> enable
Device# configure terminal
Device(config)# deploy profile unique
Device(deploy-profile-unique)# aim 0/1/1
Device(deploy-profile-unique-0/1/1)# local ranging-balance increase 2000
```

local shutdown

To configure the ONT local shutdown, use the **local shutdown** command in unique profile configuration mode. To disable the ONT local shutdown, use the **no local shutdown** command.

local shutdown {**port** *port_id* | **catv-port** *catv_port_id*}

no local shutdown {**port** *port_id* | **catv-port** *catv_port_id*}

Syntax Description

port_id	The ONT Ethernet UNI. The value range is from 1 to 24.
catv_port_id	The ONT RF interface ID. The value range is from 1 to 4.

Command Modes

Unique profile configuration (deploy-profile-unique)

Examples

This example shows how to configure the ONT local shutdown.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile unique
Device(deploy-profile-unique)# aim 0/1/1
Device(deploy-profile-unique-0/1/1)# local shutdown port 2
```

local switch

To enable the ONT local switching, use the **local switch** command in line profile configuration mode. To disable the ONT local switching, use the **no local switch** command.

local switch

no local switch

Command Modes

Line profile configuration (deploy-profile-line)

Examples

This example shows how to enable the ONT local switching.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile line
Device(deploy-profile-line)# aim 5
Device(deploy-profile-line-5)# local switch
```

ont-logging

To enable ONT logging, use the **ont-logging** command in global configuration mode. To disable ONT logging, use the **no ont-logging** command.

ont-logging

no ont-logging

Command Modes

Global configuration (config)

Examples

This example shows how to enable ONT logging.

```
Device> enable
Device# configure terminal
Device(config)# ont-logging
```

ont-logging buffer

To save the ONT log to a buffer, use the **ont-logging buffer** command in global configuration mode. To disable the ONT logging buffer, use the **no ont-logging buffer** command.

ont-logging buffer {*ont_id_list* | **all**}

no ont-logging buffer

Syntax Description

ont_id_list	The list of ONT IDs.
all	All ONTs.

Command Modes

Global configuration (config)

Examples

This example shows how to enable the ONT log buffering.

```
Device> enable
Device# configure terminal
Device(config)# ont-logging buffer all
```

ont-logging monitor

To enable monitor for ONT logs, use the **ont-logging monitor** command in global configuration mode. To disable monitor for ONT logs, use the **no ont-logging monitor** command.

ont-logging monitor {*monitor_number* | **all**} {*ont_id_list* | **all**}

no ont-logging monitor {*monitor_number* | **all**} {*ont_id_list* | **all**}

Syntax Description

monitor_number	The monitor number. The range is from 0 to 5, where 0 is the con
ont_id_list	The list of ONT IDs.
all	All ONTs.

Command Modes

Global configuration (config)

Examples

This example shows how to enable the ONT log monitor

```
Device> enable
Device# configure terminal
Device(config)# ont-logging monitor all all
```

ont-logging prefix

To configure log prefixes, use the **ont-logging prefix** command in global configuration mode. To disable log prefixing, use the **no ont-logging prefix** command.

ont-logging prefix {**ontid** | **sn**}

no ont-logging prefix

Syntax Description

ontid	The ONT IDs.
sn	The ONT serial number.

Command Modes

Global configuration (config)

Examples

This example shows how to enable the ONT log prefixing

```
Device> enable
Device# configure terminal
Device(config)# ont-logging prefix ontid
```

ont-logging timestamps

To enable log timestamps of an ONT, use the **ont-logging timestamps** command in global configuration mode.

ont-logging timestamps {**uptime** | **notime** | **datetime**}

Syntax Description

uptime	Configures logging with uptime duration.
notime	Configures logging with no time.
datetime	Configures logging with date and time

Command Modes

Global configuration (config)

Examples

This example shows how to enable log timestamps of an ONT

```
Device> enable
Device# configure terminal
Device(config)# ont-logging timestamps datetime
```

ont active

To activate the ONT, use the **ont active** *ont_id_list* command in global configuration mode.

ont active *ont_id_list*

Syntax Description

ont_id_list	The list of ONT IDs.

Command Modes

Global configuration (config)

Examples

This example show how to activate the ONT.

```
Device> enable
Device# configure terminal
Device(config)# ont active 0/1/1
Config success: 1, failed: 0.
```

Related Commands

Command	Description
ont deactive	Deactivates the ONT.

ont deactive

To deactivate the ONT, use the **ont deactive** *ont_id_list* in global configuration mode.

ont deactive *ont_id_list*

Syntax Description

ont_id_list	The list of ONT IDs.

Command Modes

Global configuration (config)

Examples

This example show how to deactivate the ONT.

```
Device> enable
Device# configure terminal
Device(config)# ont deactive 0/1/1
Config success: 1, failed: 0.
```

Related Commands

Command	Description
ont active	Activates the ONT.

ont neg-mode

To configure the ONT speed and duplex, use the **ont neg-mode speed** *speed* **duplex** *duplex_mode* *slot-num/pon-num/ont-num* **port** *port_id* command in global configuration mode.

ont neg-mode speed *speed* **duplex** *duplex_mode slot-num/pon-num/ont-num* **port** *port_id*

Syntax Description

speed	The ONT Ethernet port rate mode. The options are • 10M • 100M • 1000M • Auto-negotiation
duplex_mode	The ONT Ethernet port duplex mode. The options are • Full-duplex • Half-duplex • Auto-negotiation
slot-num/pon-num/ont-num	The ONT ID. • *slot-num*: The slot number. The value is 0. • *pon-num*: The PON number. The range is fro • *ont-num*: The ONT number. The range is fron
port_id	The ONT Ethernet port ID. The range is from 1 to

Command Modes

Global configuration (config)

Examples

This example shows how to configure the ONT speed and duplex

```
Device> enable
Device# configure terminal
Device(config)# ont neg-mode speed 10 duplex half 0/1/1 port 3
```

ont reboot

To reboot an ONT port, use the **ont reboot** command in global configuration mode.

ont reboot *slot-num/pon-num/ont-num*

Syntax Description

slot-num/pon-num/ont-num	The ONT ID. • *slot-num*: The slot number. The value is 0. • *pon-num*: The PON number. The range is fr • *ont-num*: The ONT number. The range is fr

Command Modes

Global configuration (config)

Examples

This example shows how to reboot an ONT port.

```
Device> enable
Device# configure terminal
Device(config)# ont reboot 0/1/1
```

ont shutdown

To configure the ONT shutdown, use the **ont shutdown** command in global configuration mode. To disable ONT shutdown, use the **no ont shutdown** command.

ont shutdown *slot-num/pon-num/ont-num* **port** *port_id*

no ont shutdown *slot-num/pon-num/ont-num* **port** *port_id*

Syntax Description

slot-num/pon-num/ont-num	The ONT ID. • *slot-num*: The slot number. The value is 0. • *pon-num*: The PON number. The range is from 1 • *ont-num*: The ONT number. The range is from 1
port_id	The ONT Ethernet port ID. The range is from 1 to 24.

Command Modes

Global configuration (config)

Examples

This example shows how to configure the ONT shutdown.

```
Device> enable
Device# configure terminal
Device(config)# ont shutdown 0/1/1 port 1
```

ont upgrade

To configure an ONT for reboot, use the **ont upgrade** command in global configuration mode.

ont upgrade {**auto-reboot** | **manual-reboot**} {*slot-num/pon-num/ont-num* | {**exclude** | **include**} | {**device-type** *device_type* | **software-version** *version*} | **sn** | {**string-hex** *string_serial_number* | **hex** *hex_serial_number*}}

Syntax Description

auto-reboot	Automatically reboots the ONT.
manual-reboot	Manually reboots the ONT
slot-num/pon-num/ont-num	The ONT ID. • *slot-num*: The slot number. The • *pon-num*: The PON number. Th • *ont-num*: The ONT number. Th
exclude	Excludes the ONT.
include	Includes the ONT.
device-type *device_type*	The device identifier.
software-version *version*	The software identifier.
hex_serial_number	The ONT serial number in Hex.
string_serial_number	The ONT serial number in string.

Command Modes

Global configuration (config)

Examples

This example shows how to configure an ONT fo auto reboot

```
Device> enable
Device# configure terminal
Device(config)# ont upgrade auto-reboot 0/1/1
```

optical power rx threshold

To configure the threshold of the recieve optical power, use the **optical power rx threshold** command in alarm profile configuration mode. To delete the threshold, use the **no optical power rx threshold** command.

optical power rx threshold {**high** *high_rx_power* | **low** *low_rx_power*}

no optical power rx threshold

Syntax Description

high_rx_power	The highest threshold value. The value m The unit is dBm. The range is from -127.
low_rx_power	The lowest threshold value. The value mu The unit is dBm. The range is from -127.

Command Modes

Alarm profile configuration (deploy-profile-alarm)

Examples

This example shows how to configure the high threshold value of the recieve optical power.

```
Device> enable
Device# configure terminal
Device(config)# deploy profile alarm
Device(deploy-profile-alarm)# aim 5
Device(deploy-profile-alarm-5)# optical power tx threshold high 10
```

show ont-logging

To display the ONT logs, use the **show ont-logging** command in global configuration mode

show ont-logging

Command Modes

Global configuration (config)

Examples

This example shows how to view the ONT logs

```
Device> enable
Device# configure terminal
Device(config)# show ont-logging
logging state: on
logging timestamps: uptime
logging prefix: ontid:on; sn:on
logging buffer: 0/1/1-0/8/128
logging monitor:
 0: 0/1/1-0/8/128
 1: 0/1/1-0/8/128
 2: 0/1/1-0/8/128
 3: 0/1/2-0/8/128
 4: 0/1/1-0/8/128
 5: 0/1/1-0/8/128
```

show ont-logging buffer

To display information about ONT logging buffer, use the **show ont-logging buffer** command in global configuration mode.

show ont-logging buffer {*slot-num/pon-num/ont-num* | **all**}

Syntax Description

slot-num/pon-num/ont-num	The ONT ID. • *slot-num*: The slot number. The value is 0. • *pon-num*: The PON number. The range is from • *ont-num*: The ONT number. The range is from 1
all	All ONTs

Command Modes

Global configuration (config)

Examples

This example shows how to view the information about ONT logging buffer

```
Device> enable
Device# configure terminal
Device(config)# show ont-logging buffer 0/1/1
32 day 04:28:34 0/1/1 GPON-5a946e77: offline, reason: LOSI.
32 day 04:28:34 0/1/1 GPON-5a946e77: LOAMi on.
32 day 04:28:34 0/1/1 GPON-5a946e77: LOFi on.
32 day 04:28:34 0/1/1 GPON-5a946e77: LOSi on.
32 day 04:28:31 0/1/1 GPON-5a946e77: eth port 1 los on.
32 day 02:58:03 0/1/1 GPON-5a946e77: eth port 1 los off.
32 day 02:58:00 0/1/1 GPON-5a946e77: eth port 1 los on.
31 day 23:28:51 0/1/1 GPON-5a946e77: eth port 1 los off.
31 day 23:28:47 0/1/1 GPON-5a946e77: eth port 1 los on.
26 day 07:26:06 0/1/1 GPON-5a946e77: eth port 1 los off.
26 day 07:26:04 0/1/1 GPON-5a946e77: eth port 1 los on.
26 day 04:14:38 0/1/1 GPON-5a946e77: eth port 1 los off.
26 day 04:14:36 0/1/1 GPON-5a946e77: eth port 1 los on.
26 day 03:57:30 0/1/1 GPON-5a946e77: eth port 1 los off.
26 day 03:57:27 0/1/1 GPON-5a946e77: eth port 1 los on.
26 day 03:57:15 0/1/1 GPON-5a946e77: eth port 1 los off.
25 day 05:33:41 0/1/1 GPON-5a946e77: eth port 1 los on.
25 day 05:33:31 0/1/1 GPON-5a946e77: eth port 1 los off.
25 day 05:33:30 0/1/1 GPON-5a946e77: eth port 1 los on.
24 day 23:51:33 0/1/1 GPON-5a946e77: eth port 1 los off.
24 day 23:51:30 0/1/1 GPON-5a946e77: eth port 1 los on.
24 day 23:51:17 0/1/1 GPON-5a946e77: eth port 1 los off.
21 day 08:12:36 0/1/1 GPON-5a946e77: eth port 1 los on.
21 day 08:12:28 0/1/1 GPON-5a946e77: eth port 1 los off.
!
!
!
output truncated
```

show ont mac-address-table

To display information about the MAC address table of an ONT, use the **show ont mac-address-table** command in global configuration mode.

show ont mac-address-table {*mac_address* | *slot-num/pon-num/ont-num* | **interface gpon** {*slot-number/port-number* | **all**}}

Syntax Description

mac_address	The MAC address.
slot-num/pon-num/ont-num	The ONT ID. • *slot-num*: The slot number. The value is 0. • *pon-num*: The PON number. The range is fro • *ont-num*: The ONT number. The range is fron
slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1. • 10GE Ethernet: The value is 2. • *port-number*: • GPON: The range is from 1 to 8. • GE Ethernet: The range is from 1 to 4. • 10GE Ethernet: The range is from 1 to 2.
all	All ports.

Command Modes

Global configuration (config)

Examples

This example shows how to view information about the MAC address table of an ONT

```
Device> enable
Device# configure terminal
Device(config)# show ont mac-address-table interface gpon 0/1
MAC-Address        VID  ONT-ID  SN             ID/GEM
00:0a:5a:a7:01:34  100  0/1/5   GPON-5aa7012a  4/355
Total entries: 1.
```

show ont port-status

To display status information of an ONT port, use the **show ont port-status** command in global configuration mode.

show ont port-status *slot-num/pon-num/ont-num* { **port** *port_id* | **catv-port** *catv_port_id* | **pots-port** *pots-number* }

Syntax Description

slot-num/pon-num/ont-num	The ONT ID. • *slot-num*: The slot number. The value is 0. • *pon-num*: The PON number. The range is fro • *ont-num*: The ONT number. The range is fro
port_id	The ONT Ethernet UNI. The value range is from 1 to 24.
catv_port_id	The ONT RF interface ID. The value range is from 1 to 4.
pots-number	Specifies the POTS port. The value can be 1 or 2.

Command Modes

Global configuration (config)

Examples

This example shows how to view the status information of an ONT port.

```
Device> enable
Device# configure terminal
Device(config)# show ont port-status 0/1/5 port 2
Port status is Enable, Linkdown
```

show ont statistics

To display statistical information about an ONT, use the **show ont statistics** command in global configuration mode.

show ont statistics *slot-num/pon-num/ont-num* {**gem** {**broadcast** | **multicast** | **unicast** *gem_index* } | {**port** *port-id* } | **traffic**}

Syntax Description

slot-num/pon-num/ont-num	The ONT ID. • *slot-num*: The slot number. The value is 0. • *pon-num*: The PON number. The range is fi • *ont-num*: The ONT number. The range is fr
gem	Displays statistical information about GEM port
broadcast	Displays statistical information about broadcast
multicast	Displays statistical information about multicast p
unicast *gem_index*	Displays statistical information about unicast pa *gem_index* : The GEM port index number. The r
port-id	The ONT Ethernet port ID. The range is from 1 to 24.
traffic	Displays statistical information about ONT upli

Command Modes

Global configuration (config)

Examples

This example shows how to view the statistical information about an ONT.

```
Device> enable
Device# configure terminal
Device(config)# show ont statistics 0/1/1 port 1
Upstream frames : 0
Upstream bytes : 0
Downstream frames : 0
Downstream bytes : 0
Up traffic (kbps) : 0
Down traffic (kbps) : 0
```

show ont upgrade-status

To display the ONT upgrade status, use the **show ont upgrade-status** command in global configuration mode.

show ont upgrade-status {**image** | **xml**} {*slot-num/pon-num/ont-num* | **all**}

Syntax Description

slot-num/pon-num/ont-num	The ONT ID. • *slot-num*: The slot number. The value is 0. • *pon-num*: The PON number. The range is from 1 • *ont-num*: The ONT number. The range is from 1
all	All ports.

Command Modes

Global configuration (config)

Examples

This example shows how to view the ONT upgrade status

```
evice> enable
Device# configure terminal
Device(config)# show ont upgrade-status image 0/1/1
ONT   Active-version Inactive-version Status
0/1/1 C01R544V00B09  C01R544V00B07    success
Total entries: 1.
```

show ont version

To display an ONT version, use the **show ont version** command in global configuration mode.

show ont version interface gpon {*port_list* | **all**}

Syntax Description

port_list	The GPON port.
all	All ports.

Command Modes

Global configuration (config)

Examples

This example shows how to view an ONT version

```
Device> enable
Device# configure terminal
Device(config)# show ont version interface gpon 0/1
ONT    SN              Software-version          Firmware-version
0/1/1  GPON-5a946e77   B01D001P010/B01D001P008   N40-428-1
0/1/2  GPON-5a95efca   C01R539V00B19/-           S40-401
0/1/3  GPON-5aa0e950   B01D001P010/B01D001P007   N40-428-1
0/1/4  GPON-5aa0e9e0   B01D001P007/B01D001P006   N40-428-1
0/1/5  GPON-5aa7012a   1.1.2.5/1.1.2.6           N40-428-1
Total entries: 5.
```