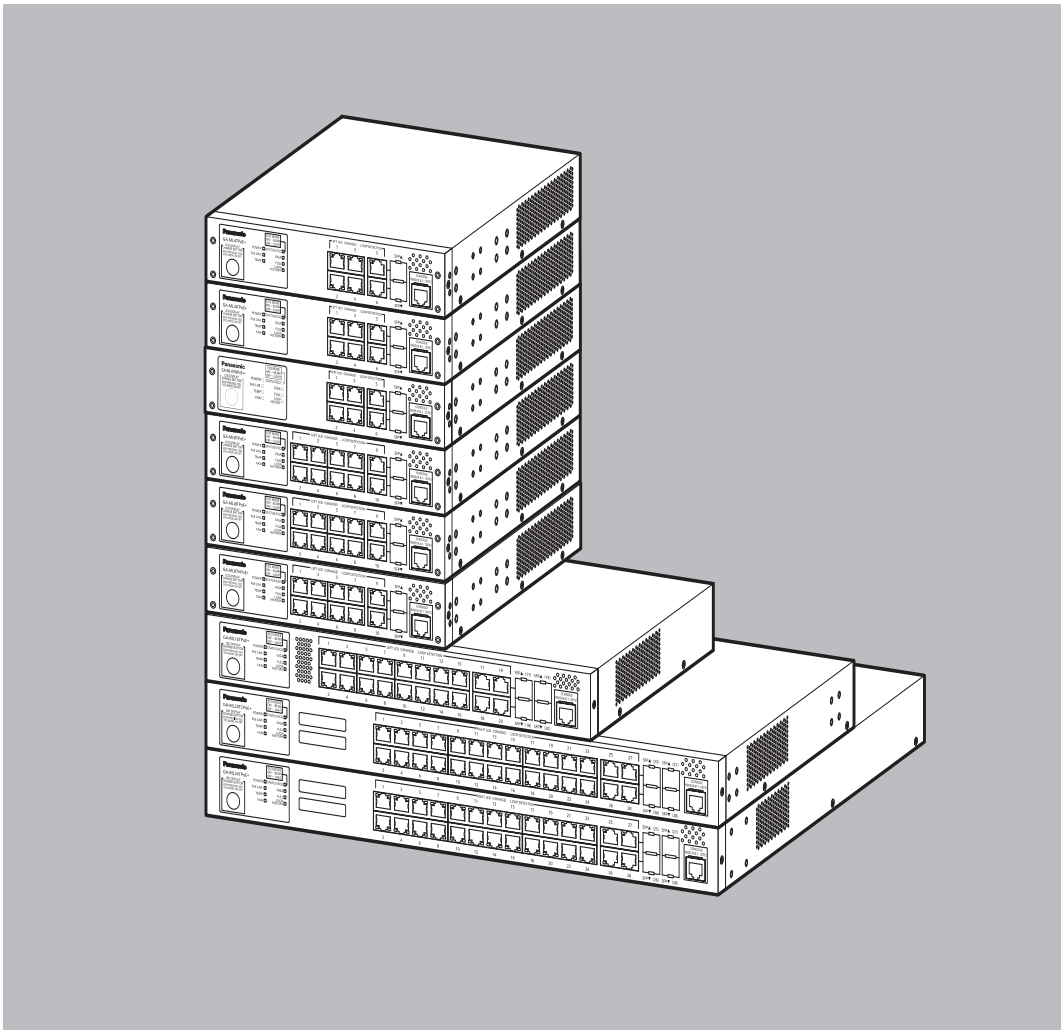
Panasonic

GA-ML Series

CLI Reference

Model Number PN260493N/PN260493H/PN260496/
PN260893/PN260893H/PN260894/
PN261693/PN262492/PN262493



The target model for this CLI reference is as follows

Model Name	Model Number	Firmware Version
GA-ML4TPoE+	PN260493N	3.1.0.04 or higher
GA-MLi4TPoE+	PN260493H	3.1.0.04 or higher
GA-ML4TWPoE++	PN260496	3.1.0.04 or higher
GA-ML8TPoE+	PN260893	3.1.0.04 or higher
GA-MLi8TPoE+	PN260893H	3.1.0.04 or higher
GA-ML8THPoE+	PN260894	3.1.0.04 or higher
GA-ML16TPoE+	PN261693	3.1.0.04 or higher
GA-ML24TCPoE+	PN262492	3.1.0.04 or higher
GA-ML24TPoE+	PN262493	3.1.0.04 or higher

Table of Contents

1 Getting Started

1.1 Introduction

The commands listed here are the subset of commands that are supported by the GA-ML Series Gigabit Ethernet Switch.

1.1.1 Intended Readers

This reference manual is intended for network administrators and other IT networking professionals responsible for managing the switch by using the Command Line Interface (CLI). The CLI is the primary management interface to the GA-ML series switch, which will be generally be referred to simply as the "Switch" within this manual. This manual is written in a way that assumes that you already have experience with and knowledge of Ethernet and modern networking principles for Local Area Networks.

1.1.2 Typographic Conventions

Convention	Description
Boldface Font	This convention is used to place emphasis on keywords. It also indicates commands and command options. Keywords, in the command line, are to be entered exactly as they are displayed.
UPPERCASE ITALICS Font	Parameters or values that must be specified are printed in *UPPERCASE ITALICS*. Parameters in the command line are to be replaced with the actual values that are desired to be used with the command.
Square Brackets [ ]	Square brackets enclose an optional value or set of optional arguments.
Braces { }	Braces enclose alternative keywords separated by vertical bars. Generally, one of the keywords in the separated list can be chosen.
Vertical Bar |	Optional values or arguments are enclosed in square brackets and separated by vertical bars. Generally, one or more of the vales or arguments in the separated list can be chosen.
`Courier Font`	This convention is used to represent a Command Line Interface (CLI) example. All examples used in this manual are based on the GA-ML switch in the Series.

1.1.3 Notes and Cautions

NOTE A note indicates important information that helps you make better use of your device.

⚠ CAUTION A caution indicates a potential for property damage, personal injury, or death.

1.1.4 Command Descriptions

The information pertaining to each command in this reference guide is presented using a number of template fields. The fields are:

- Description - This is a short and concise statement describing the functionality of the command.
- Syntax - The precise form to use when entering and issuing the command.
- Parameters - A table where each row describes the optional or required parameters, and their use, that can be issued with the command.
- Default - If the command sets a configuration value or administrative state of the Switch then any default settings (i.e. without issuing the command) of the configuration is shown here.
- Command Mode - The mode in which the command can be issued. These modes are described in the section titled “Command Modes” below.
- Command Default Level - The user privilege level in which the command can be issued.
- Usage Guidelines - If necessary, a detailed description of the command and its various utilization scenarios is given here.
- Example(s) - Each command is accompanied by a practical example of the command being issued in a suitable scenario.

1.1.5 Command Modes

There are several command modes available in the command-line interface (CLI). The set of commands available to the user depends on both the mode the user is currently in and their privilege level. For each case, the user can see all the commands that are available in a particular command mode by entering a question mark (?) at the system prompt.

The command-line interface has five pre-defined privilege levels:

- Basic User - Privilege Level 1. This user account level has the lowest priority of the user accounts. The purpose of this type of user account level is for basic system checking.

- Advanced User - Privilege Level 3. This user account level is allowed to configure the terminal control setting. This user account can only show limited information that is not related to security.
- Power User - Privilege 8. This user account level can execute fewer commands than operator, including configuration commands other than the operator level and administrator level commands.
- Operator - Privilege Level 12. This user account level is used to grant system configuration rights for users who need to change or monitor system configuration, except for security related information such as user accounts and SNMP account settings, etc.
- Administrator - Privilege Level 15. This administrator user account level can monitor all system information and change any of the system configuration settings expressed in this configuration guide.

The command-line interface has a number of command modes. There are three basic command modes:

- User EXEC Mode
- Privileged EXEC Mode
- Global Configuration Mode

All other sub-configuration modes can be accessed via the Global Configuration Mode.

When a user logs in to the Switch, the privilege level of the user determines the command mode the user will enter after initially logging in. The user will either log into User EXEC Mode or the Privileged EXEC Mode.

- Users with a basic user level will log into the Switch in the User EXEC Mode.
- Users with advanced user, power-user, operator or administrator level accounts will log into the Switch in the Privileged EXEC Mode.

Therefore, the User EXEC Mode can operate at a basic user level and the Privileged EXEC Mode can operate at the advanced user, power-user, operator, or administrator levels. The user can only enter the Global Configuration Mode from the Privileged EXEC Mode. The Global Configuration Mode can be accessed by users who have operator or administrator level user accounts.

As for sub-configuration modes, a subset of those can only be accessed by users who have the highest secure administrator level privileges.

The following table briefly lists the available command modes. Only the basic command modes and some of the sub-configuration modes are enumerated. The basic command modes and basic sub-configuration modes are further described in the following chapters. Descriptions for the rest of the sub-configuration modes are not provided in this section. For more information on the additional sub-configuration modes, the user should refer to the chapters relating to these functions.

The available command modes and privilege levels are described below:

Command Mode/ Privilege Level	Purpose
User EXEC Mode / Basic User level	This level has the lowest priority of the user accounts. It is provided only to check basic system settings.
Privileged EXEC Mode / Advanced User level	This level is allowed to configure the terminal control setting. This user account can only show limited information that is not related to security.
Privileged EXEC Mode / Power User level	This level can execute less commands than operator, including the 'config' commands other than the operator level and administrator level commands.
Privileged EXEC Mode / Operator level	For changing local and global terminal settings, monitoring, and performing certain system administration tasks. Except for security related information, this level can perform system administration tasks.
Privileged EXEC Mode / Administrator level	This level is identical to privileged EXEC mode at the operator level, except that a user at the administrator level can monitor and clear security related settings.
Global Configuration Mode / Operator level	For applying global settings, except for security related settings, on the entire switch. In addition to applying global settings on the entire switch, the user can access other sub-configuration modes from global configuration mode.
Global Configuration Mode / Administrator level	For applying global settings on the entire switch. In addition to applying global settings on the entire switch, the user can access other sub-configuration modes from global configuration mode.
Interface Configuration Mode / Administrator level	For applying interface related settings.
VLAN Interface Configuration Mode	For applying VLAN interface related settings.

User EXEC Mode at Basic User Level

This command mode is mainly designed for checking basic system settings. This command mode can be entered by logging in as a basic user.

Privileged EXEC Mode at Advanced User Level

This command mode is mainly designed for checking basic system settings, allowing users to change the local terminal session settings and carrying out basic network connectivity verification. One limitation of this command mode is that it cannot be used to display information related to security. This command mode can be entered by logging in as an advanced user.

Privileged EXEC Mode at Power User Level

Users logged into the Switch in privileged EXEC mode at this level can execute fewer commands than operators, including the 'config' commands other than the operator level and administrator level commands. The method to enter the privileged EXEC mode at the power user level is to log into the Switch with a user account that has a privilege level of 8.

Privileged EXEC Mode at Operator Level

Users logged into the Switch in privileged EXEC mode at this level can change both local and global terminal settings, monitor, and perform system administration tasks (except for security related information). The method to enter privileged EXEC mode at operator level is to log into the Switch with a user account that has a privilege level of 12.

Privileged EXEC Mode at Administrator Level

This command mode has a privilege level of 15. Users logged in with this command mode can monitor all system information and change any system configuration settings mentioned in this Configuration Guide. The method to enter privileged EXEC mode at administrator level is to log into the Switch with a user account that has a privilege level of 15.

Global Configuration Mode

The primary purpose of the global configuration mode is to apply global settings to the entire switch. The global configuration mode can be accessed through advanced user, power user, operator or administrator level user accounts. However, security related settings are not accessible through advanced user, power user or operator user accounts. In addition to applying global settings to the entire switch, the user can also access other sub-configuration modes. In order to access the global configuration mode, the user must be logged in with the corresponding account level and use the **configure terminal** command in the privileged EXEC mode.

In the following example, the user is logged in as an Administrator in the Privileged EXEC Mode and uses the **configure terminal** command to access the Global Configuration Mode:

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)#
```

The **exit** command is used to exit the global configuration mode and return to the privileged EXEC mode.

```
GA-MLxxTPoE+(config)# exit
GA-MLxxTPoE+#
```

The procedures to enter the different sub-configuration modes can be found in the related chapters in this Configuration Guide. The command modes are used to configure the individual functions.

Interface Configuration Mode

Interface configuration mode is used to configure the parameters for an interface or a range of interfaces. An interface can be a physical port, VLAN, or other virtual interface. Thus, interface configuration mode is distinguished further according to the type of interface. The command prompt for each type of interface is slightly different.

VLAN Interface Configuration Mode

VLAN interface configuration mode is one of the available interface modes and is used to configure the parameters of a VLAN interface.

To access VLAN interface configuration mode, use the following command in global configuration mode:

```
GA-MLxxTPoE+(config)# interface vlan 1
GA-MLxxTPoE+(config-if)#
```

1.1.6 Creating a User Account

By default, there is no user account created on this switch. For security reasons, it is highly recommended to create user accounts to manage and control access to this switch's interface. This section will assist a user with creating a user account by means of the Command Line Interface.

Observe the following example.

```
GA-MLxxTPoE+# enable
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# username admin password admin
GA-MLxxTPoE+(config)# username admin privilege 15
GA-MLxxTPoE+(config)# line console
GA-MLxxTPoE+(config-line)# login local
GA-MLxxTPoE+(config-line)#
```

In the above example we had to navigate and access the username command.

- Starting in the User EXEC Mode, we enter the **enable** command to access the Privileged EXEC Mode.
- After accessing the Privileged EXEC Mode, we entered the **configure terminal** command to access the Global Configuration Mode. The **username** command can be used in the Global Configuration Mode.
- The **username admin password admin** command creates a user account with the username of admin and a password of admin.
- The **username admin privilege 15** command assigns a privilege level value of 15 to the user account admin.
- The **line console** command allows us to access the console interface's Line Configuration Mode.
- The **login local** command tells the Switch that users need to enter locally configured login credentials to access the console interface.

Save the running configuration to the start-up configuration. This means to save the changes made so that when the Switch is rebooted, the configuration will not be lost. The following example shows how to save the running configuration to the start-up configuration.

```
GA-MLxxTPoE+# copy running-config startup-config

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

GA-MLxxTPoE+#
```

After the Switch has rebooted, or after the users log out and back in, the newly created username and password must be entered to access the CLI interface again, as seen below.

```
                GA-MLxxTPoE+ Gigabit Ethernet Switch

                     Command Line Interface
                   Firmware: Build V2.0.1.02
                  Serial Number: xxxxxxxxxxx

User Access Verification

Username:admin
Password:*****

GA-MLxxTPoE+#
```

1.1.7 Interface Notation

When configuring the physical ports available on this switch, a specific interface notation is used. The following will explain the layout, terminology and use of this notation.

In the following example, we'll enter the Global Configuration Mode and then enter the Interface Configuration Mode, using the notation 1/0/1. After entering the Interface Configuration Mode for port 1, we'll change the speed to 1 Gbps, using the speed 1000 command.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# speed 1000
GA-MLxxTPoE+(config-if)#
```

In the above example the notation 1/0/1 was used. The terminology for each parameter is as follows:

- Interface Unit's ID / Open Slot's ID / Port's ID

The Interface Unit's ID is one always.
The Open Slot's ID is zero.
Lastly, the Port's ID is the physical port number of the port being configured.

1.1.8 Error Messages

When users issue a command that the Switch does not recognize, error messages will be generated to assist users with basic information about the mistake that was made. A list of possible error messages are found in the table below.

Error Message	Meaning
Ambiguous command	Not enough keywords were entered for the Switch to recognize the command.
Incomplete command	The command was not entered with all the required keyword.
Invalid input detected at ^marker	The command was entered incorrectly.

The following example shows how an ambiguous command error message is generated.

```
GA-MLxxTPoE+# show v
Ambiguous command
GA-MLxxTPoE+#
```

The following example shows how an incomplete command error message is generated.

```
GA-MLxxTPoE+# show
Incomplete command
GA-MLxxTPoE+#
```

The following example shows how an invalid input error message is generated.

```
GA-MLxxTPoE+# show verb
             ^
Invalid input detected at ^marker
GA-MLxxTPoE+#
```

1.1.9 Editing Features

The command line interface of this switch supports the following keyboard keystroke editing features.

Keystroke	Description
Delete	Deletes the character under the cursor and shifts the remainder of the line to the left.
Backspace	Deletes the character to the left of the cursor and shifts the remainder of the line to the left.
Left Arrow	Moves the cursor to the left.

Keystroke	Description
Right Arrow	Moves the cursor to the right.
CTRL+R	Toggles the insert text function on and off. When on, text can be inserted in the line and the remainder of the text will be shifted to the right. When off, text can be inserted in the line and old text will automatically be replaced with the new text.
Return	Scrolls down to display the next line or used to issue a command.
Space	Scrolls down to display the next page.
ESC	Escapes from the displaying page.

2 Management

2.1 Basic CLI Commands

2.1.1 help

This command is used to display a brief description of the help system. Use the help command in any command mode.

Syntax

- help

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode
Any Configuration Mode

Command Default Level

Level: 1

Usage Guideline

The help command provides a brief description for the help system, which includes the following functions:

- To list all commands available for a particular command mode, enter a question mark (?) at the system prompt.
- To obtain a list of commands that begin with a particular character string, enter the abbreviated command entry immediately followed by a question mark (?). This form of help is called word help, because it lists only the keywords or arguments that begin with the abbreviation entered.

- To list the keywords and arguments associated with a command, enter a question mark (?) in place of a keyword or argument on the command line. This form of help is called the **command syntax** help, because it lists the keywords or arguments that apply based on the command, keywords, and arguments already entered.

Example

This example shows how the help command is used to display a brief description of the help system.

```
GA-MLxxTPoE+#help

The switch CLI provides advanced help feature.
1. Help is available when you are ready to enter a command
   argument (e.g. 'show ?') and want to know each possible
   available options.
2. Help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input(e.g. 'show ve?'.).
   If nothing matches, the help list will be empty and you must backup
   until entering a '?' shows the available options.
3. For completing a partial command name could enter the abbreviated
   command name immediately followed by a <Tab> key.

Note:
Since the character '?' is used for help purpose, to enter
the character '?' in a string argument, press ctrl+v immediately
followed by the character '?'.


GA-MLxxTPoE+#
```

The following example shows how to use the **word** help to display all the Privileged EXEC Mode commands that begin with the letters “re”. The letters entered before the question mark (?) are reprinted on the next command line to allow the user to continue entering the command.

```
GA-MLxxTPoE+#re?
reboot   rename   renew   replace   reset

GA-MLxxTPoE+#re
```

The following example shows how to use the **command syntax** help to display the next argument of a partially complete **enable** command. The characters entered before the question mark (?) are reprinted on the next command line to allow the user to continue entering the command.

```
GA-MLxxTPoE+#enable ?
 <1-15>  <privilege 1-15>
 <CR>    Carriage return

GA-MLxxTPoE+#enable
```

2.1.2 enable

This command is used to change the privilege level of the active CLI login session.

Syntax

- **enable** [*PRIVILEGE-LEVEL*]

Parameters

Parameters	Description
PRIVILEGE-LEVEL	(Optional) Specifies the privilege level. The range is from 1 to 15. If not specified, privilege level 15 will be used.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

If the privileged level requires a password, enter it in the field provided. Only three attempts are allowed. Failure to access this level returns the user to the current level.

Example

This example shows how to change the privilege level of the active CLI login session to privilege level 15.

```
GA-MLxxTPoE+#enable 15
password:******
GA-MLxxTPoE+#
```

2.1.3 disable

This command is used to change the privilege level of the active CLI login session to a lower privilege level.

Syntax

- disable [*PRIVILEGE-LEVEL*]

Parameters

Parameters	Description
PRIVILEGE-LEVEL	(Optional) Specifies the privilege level. If not specified, privilege level 1 will be used.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command is used to change the privilege level of the active CLI login session to a lower privilege level. When using this command to enter a privilege level that requires password, there is no need to enter the password.

Example

This example shows how to change the privilege level of the active CLI login session to privilege level 1.

```
GA-MLxxTPoE+#show privilege

Current privilege level is 15

GA-MLxxTPoE+#disable 1
GA-MLxxTPoE+> show privilege

Current privilege level is 1

GA-MLxxTPoE+>
```

2.1.4 configure terminal

This command is used to enter the Global Configuration Mode.

Syntax

- configure terminal

Parameters

None

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to enter the Global Configuration Mode.

Example

This example shows how to enter the Global Configuration Mode.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#
```

2.1.5 login (EXEC)

This command is used to configure a login username.

Syntax

- login

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to change the login account. Three attempts are allowed to log into the Switch's interface. When using Telnet, if all attempts fail, access will return to the command prompt. If no information is entered within 60 seconds, the session will return to the state when logged out.

Example

This example shows how to login with username "user1".

```
GA-MLxxTPoE+> login

UserName:manager
Password:*******

GA-MLxxTPoE+>
```

2.1.6 login (Line)

This command is used to set the line login method. Use the **no** form of this command to disable the login.

Syntax

- **login [local]**
- **no login**

Parameters

Parameters	Description
local	(Optional) Specifies that the line login method will be local.

Default

By default, Username and Password are set manager and manager for the **console** line.

By default, there is a login method (by password) configured for the **Telnet** line.
By default, there is a login method (by password) configured for the **SSH** line.

Command Mode

Line Configuration Mode

Command Default Level

Level: 15

Usage Guideline

For Console and Telnet access, when AAA is enabled, the line uses rules configured by the AAA module. When AAA is disabled, the line uses the following authentication rules:

- When login is disabled, the user can enter the line at Level 1.
- When the **by password** option is selected, after inputting the same password as the **password** command, the user will enter the line at level 1. If the password wasn't previously configured, an error message will be displayed and the session will be closed.
- When the **username and password** option is selected, enter the username and password configured by the **username** command.

For SSH access, there are three authentication types:

- SSH public key
- Host-based authentication
- Password authentication

The SSH public key and host-based authentication types are independent from the login command in the line mode. If the authentication type is password, the following rules apply:

- When AAA is enabled, the AAA module is used.
- When AAA is disabled, the following rules are used:
  - When login is disabled, the username and password are ignored. Enter the details at Level 1.
  - When the **username and password** option is selected, enter the username and password configured by the **username** command.
  - When the **password** option is selected, the username is ignored but a password is required using the **password** command to enter the line at level 1.

Example

This example shows how to enter the Line Configuration Mode and to create a password for the line user. This password only takes effect once the corresponding line is set to login.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#line console
GA-MLxxTPoE+(config-line)#password loginpassword
GA-MLxxTPoE+(config-line)#
```

This example shows how to configure the line console login method as “login”.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#line console
GA-MLxxTPoE+(config-line)#login
GA-MLxxTPoE+(config-line)#
```

This example shows how to create a username “useraccount” with the password of “pass123” and use Privilege 12.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#username useraccount privilege 12 password 0 pass123
GA-MLxxTPoE+(config)#
```

This example shows how to configure the login method as login local.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#line console
GA-MLxxTPoE+(config-line)#login local
GA-MLxxTPoE+(config-line)#
```

2.1.7 logout

This command is used to close an active terminal session by logging off the Switch.

Syntax

- logout

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level:1

Usage Guideline

Use this command to close an active terminal session by logging out of the device.

Example

This example shows how to log out.

```
GA-MLxxTPoE+#logout
```

2.1.8 end

This command is used to end the current configuration mode and return to the highest mode in the CLI mode hierarchy, which is either the User EXEC Mode or the Privileged EXEC Mode.

Syntax

- **end**

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode
Any Configuration Mode

Command Default Level

Level: 1

Usage Guideline

Executing this command will return access to the highest mode in the CLI hierarchy.

Example

This example shows how to end the Interface Configuration Mode and go back to the Privileged EXEC Mode.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#end
GA-MLxxTPoE+#
```

2.1.9 exit

This command is used to end the configuration mode and go back to the last mode. If the current mode is the User EXEC Mode or the Privileged EXEC Mode, executing the exit command logs you out of the current session.

Syntax

- exit

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode
Any Configuration Mode.

Command Default Level

Level: 1

Usage Guideline

Use this command to exit the current configuration mode and go back to the last mode. When the user is in the User EXEC Mode or the Privileged EXEC Mode, this command will log out the session.

Example

This example shows how to exit from the Interface Configuration Mode and return to the Global Configuration Mode.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#exit
GA-MLxxTPoE+(config)#
```

2.1.10 show history

This command is used to list the commands entered in the current EXEC Mode session.

Syntax

- show history

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Commands entered are recorded by the system. A recorded command can be recalled in sequence by pressing CTRL+P or the Up Arrow key. The history buffer size is fixed at 20 commands.

The function key instructions below display how to navigate the commands in the history buffer.

- CTRL+P or the Up Arrow key - Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
- CTRL+N or the Down Arrow key - Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow key. Repeat the key sequence to recall successively more recent commands.

Example

This example shows how to display the command buffer history.

```
GA-MLxxTPoE+#show history

 help
 history

GA-MLxxTPoE+#
```

2.1.11 show environment

This command is used to display fan, temperature, power availability and status information.

Syntax

- **show environment [fan | power | temperature]**

Parameters

Parameters	Description
fan	(Optional) Specifies to display the detailed fan status.
power	(Optional) Specifies to display the detailed power status.
temperature	(Optional) Specifies to display the detailed temperature status.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

If a specific type is not specified, all types of environment information will be displayed.

Example

This example shows how to display fan, temperature, power availability, and status information.

```
GA-MLxxTPoE+>show environment

Detail Temperature Status:
Unit     Temperature Descr/ID          Current/Threshold Range
-----   ------------------------------------------------------
1        Thermal Sensor/1              35/69C
1        Thermal Sensor/2              35/68C
Status code: * temperature is out of threshold range

Detail Fan Status:
-------------------------------------------------------------
Unit 1:
Back Fan  1 : Speed High
Back Fan  2 : Speed High

Detail Power Status:
Unit    Power Module      Power Status
-----   ----------------  -------------
1       Power 1           In-operation

GA-MLxxTPoE+>
```

2.1.12 show unit

This command is used to display information about system units.

Syntax

- **show unit** [*UNIT-ID*]

Parameters

Parameters	Description
UNIT-ID	(Optional) Specify the unit to display.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command displays information about the system modules. If no parameter is specified, information of all units will be displayed.

Example

This example shows how to display the information about units on a system.

```
GA-MLxxTPoE+>show unit

Unit: 1
Model Descr: 8P 10/100/1000 with 2P Combo
Product Name: GA-MLxxTPoE+
Product Number: PNxxxxxx
Serial-Number: xxxxxxxxxxx
Status: OK
Up Time: 0DT1H53M57S
DRAM        495832 K total,     277868 K used,     217964 K free
FLASH        92780 K total,      33904 K used,      58876 K free

GA-MLxxTPoE+>
```

2.1.13 show cpu utilization

This command is used to display the CPU utilization information.

Syntax

- **show cpu utilization**

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command displays the system's CPU utilization information in 5 second, 1 minute, and 5 minute intervals.

Example

This example shows how to display the CPU utilization information.

```
GA-MLxxTPoE+#show cpu utilization

CPU Utilization

Five seconds -  35 %         One minute -  33 %         Five minutes -  33 %


GA-MLxxTPoE+#
```

2.1.14 show version

This command is used to display the version information of the Switch.

Syntax

- show version

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display the version information of the Switch.

Example

This example shows how to display the version information of the Switch.

```
GA-MLxxTPoE+#show version

System MAC Address: 00-50-40-xx-xx-xx

Unit ID    Module Name                    Versions
-------  ---------------------------  --------------------
   1      GA-MLxxTPoE+                 H/W:A1
                                       Bootloader:V1.0.0.05
                                       Runtime:V2.0.1.00


GA-MLxxTPoE+#
```

2.1.15 show memory utilization

This command is used to display the memory utilization information.

Syntax

- **show memory utilization**

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command displays the system's memory utilization information.

Example

This example shows how to display the information about memory utilization.

```
GA-MLxxTPoE+#show memory utilization

Unit: 1
DRAM      524288 K total,   217038 K used,   307250 K free
FLASH     122368 K total,    47112 K used,    75256 K free

GA-MLxxTPoE+#
```

2.1.16 show privilege

This command is used to display the current privilege level.

Syntax

- **show privilege**

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display the current privilege level.

Example

This example shows how to display the current privilege level.

```
GA-MLxxTPoE+#show privilege

Current privilege level is 15

GA-MLxxTPoE+#
```

2.2 Access Management Commands

2.2.1 access class

This command is used to specify an access list to restrict the access via a line. Use the **no** form of this command to remove the specified access list check.

Syntax

- **access-class** *IP-ACL*
- **no access-class** *IP-ACL*

Parameters

Parameters	Description
IP-ACL	Specifies a standard IP access list. The source address field of the permit or deny entry define the valid or invalid host.

Default

None

Command Mode

Line Configuration Mode

Command Default Level

Level: 15

Usage Guidelines

This command specifies access lists to restrict the access via a line. At most two access lists can be applied to a line. If two access lists are already applied, an attempt to apply a new access list will be rejected until an applied access list is removed by the **no** form of this command.

Example

This example shows how a standard IP access list is created and is specified as the access list to restrict access via Telnet. Only the host 226.1.1.1 is allowed to access the server.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#ip access-list vty_filter
GA-MLxxTPoE+(config-ip-acl)#permit 226.1.1.1 0.0.0.0
GA-MLxxTPoE+(config-ip-acl)#exit
GA-MLxxTPoE+(config)#line telnet
GA-MLxxTPoE+(config-line)#access-class vty_filter
GA-MLxxTPoE+(config-line)#
```

2.2.2 prompt

This command is used to customize the CLI prompt. Use the **no** form of this command to revert to the default setting.

Syntax

- **prompt** *STRING*
- **no prompt**

Parameters

Parameters	Description
STRING	Specifies a string to define the customized prompt. The prompt will be based on the specified characters or the following control characters. The space character in the string is ignored. **% h** – encode the Product name. **%s** – space **%%** - encode the % symbol

Default

By default, the string encodes the Product name (GA-MLxxTPoE+).

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use this command to customize the CLI prompt. If the user selects to encode the Product name as the prompt, only the first 15 characters are encoded. The prompt can only display up to 15 characters. The privileged level character will appear as the last character of the prompt.
The character is defined as follows.

- **>** - Represents user level.
- **#** - Represents privileged user level.

Example

The following example describes how to change the prompt to "BRANCH A" using administrator.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#prompt BRANCH%sA
BRANCH A(config)#
```

2.2.3 enable password

This command is used to setup enable password to enter different privileged levels and use the **no** to return the password to the empty string.

Syntax

- **enable password [level** *PRIVILEGE-LEVEL*] [0 | 7] *PASSWORD*
- **no enable password [level** *PRIVILEGE-LEVEL*]

Parameters

Parameters	Description
level *PRIVILEGE-LEVEL*	(Optional) Specifies the privilege level for the user. The privilege level is between 1 and 15. If this argument is not specified in the command or the no form of the command, the privilege level defaults to 15 (traditional enable privileges).
0	(Optional) Specifies the password in clear, plain text. The password length is between 1 and 32 characters and can contain embedded spaces. It is case-sensitive. If the password syntax cannot be specified, the syntax remains plain text.

Parameters	Description
7	(Optional) Specifies the encrypted password based on SHA-1. The password length is fixed at 35 bytes. It is case-sensitive. The password is encrypted. If the password syntax is not specified, the syntax is plain text.
PASSWORD	Specifies the password for the user.

Default

By default, no password is set. It is an empty string.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guidelines

The exact password for a specific level needs to be used to enter the privilege level. Each level has only one password to enter the level.

Example

The following example describes how to create an **enable** password at the privilege level 15 of "MyEnablePassword".

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#enable password MyEnablePassword
GA-MLxxTPoE+#
```

2.2.4 ip http server

Use this command to enable an HTTP server. To disable the HTTP server function, use the **no** form of the command.

Syntax

- **ip http server**
- **no ip http server**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use the command above to enable the HTTP server function. Regarding an HTTP access interface, it is controlled by using the SSL command.

Example

The following example describes how to enable the HTTP server.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip http server
GA-MLxxTPoE+(config)#
```

2.2.5 ip http secure-server

Use this command to enable an HTTPS server. Use the command of **ip http secure-server sslservice-policy** to specify the SSL service policy, which is used for HTTPS. To disable a function of the HTTPS server, use **no** form of the command.

Syntax

- **ip http secure-server [ssl-service-policy** *POLICY-NAME*]
- **no ip http secure-server**

Parameters

Parameters	Description
ssl-service-policy *POLICY-NAME*	Specify the name of an SSL service policy (Optional). Regarding the **ssl-service-policy** parameter, it is used if the **ssl-service-policy** command is used and the SSL service policy is declared, already.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

With the command above, enable the HTTPS server function. Then use the SSL service policy specified for HTTPS. If you do not specify the option parameter, use the built-in local certificate for the HTTPS.

Example

The following example describes how to use the service policy called “sp1” for HTTPS by enabling the HTTPS server function.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip http secure-server ssl-service-policy sp1
GA-MLxxTPoE+(config)#
```

2.2.6 ip http access-class

Use this command to specify the access-list to control accesses to an HTTP server. To delete the access-list check, use **no** form of the command.

Syntax

- **ip {http | https} access-class** *IP-ACL*
- **no ip {http | https} access-class** *IP-ACL*

Parameters

Parameters	Description
IP-ACL	Specify the standard IP access-list. In the field of source-address of an entry, define an enabled or disabled host.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use the command above to specify the access-list, which controls accesses to an HTTP server. If the access-list specified does not exist, then the command is not enabled; checking access-lists is not conducted when users access the HTTP.

Example

The following example describes how to specify as the access list, which allows you to access HTTP servers by creating a standard IP access list. Only host 226.1.1.1 is allowed to access the servers.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip access-list http-filter
GA-MLxxTPoE+(config-ip-acl)# permit 226.1.1.1 0.0.0.0
GA-MLxxTPoE+(config-ip-acl)# exit
GA-MLxxTPoE+(config)# ip http access-class http-filter
GA-MLxxTPoE+(config)#
```

2.2.7 ip http service-port

Use this command to specify the HTTP service port. To return to the default settings, use **no** form of the command.

Syntax

- **ip http service-port** *TCP-PORT*

- no ip http service-port

Parameters

Parameters	Description
TCP-PORT	Specify the TCP port-number. For the TCP port-number, specify it using the value: the range is from 1 to 65,535. The TCP port, which is used for the HTTP protocol is 80th of "well-known ports".

Default

By default, this port-number is 80.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use the command to configure the TCP port-number of the HTTP server.

Example

The following example describes how to set the HTTP TCP port-number to 8,080.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip http service-port 8080
GA-MLxxTPoE+(config)#
```

2.2.8 ip http timeout-policy idle

- To return to the default settings, use no form of the command above.

Syntax

- ip http timeout-policy idle INT
- no ip http timeout-policy idle

Parameters

Parameters	Description
INT	This parameter specifies the value of idle time-out. The valid range is between 60 and 36,000 (seconds).

Default

By default, the value is set to 180 (seconds).

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use the command above to configure the value of idle time-out of the HTTP server connection.

Example

The following example describes how to set the value of idle time-out to 100 (seconds).

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip http timeout-policy idle 100
GA-MLxxTPoE+(config)#
```

2.2.9 ip telnet server

This command is used to enable a Telnet server. Use the **no** form of this command to disable the Telnet server function.

Syntax

- **ip telnet server**
- **no ip telnet server**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

This command enables or disables the Telnet server. The SSH access interface is separately controlled by SSH commands.

Example

This example describes how to enable the Telnet server.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#ip telnet server
GA-MLxxTPoE+(config)#
```

2.2.10 ip telnet service-port

This command is used to specify the service port for Telnet. Use the **no** form of this command to revert to the default setting.

Syntax

- **ip telnet service-port** *TCP-PORT*
- **no ip telnet service-port**

Parameters

Parameters	Description
TCP-PORT	Specifies the TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port for the Telnet protocol is 23.

Default

By default, this value is 23.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

This command configures the TCP port number for Telnet access.

Example

This example shows how to change the Telnet service port number to 3000.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#ip telnet service-port 3000
GA-MLxxTPoE+(config)#
```

2.2.11 line

This command is used to identify a line type for configuration and enter line configuration mode.

Syntax

- **line {console | telnet | ssh}**

Parameters

Parameters	Description
console	Specifies the local console terminal line.
telnet	Specifies the Telnet terminal line.
ssh	Specifies the SSH terminal line.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

The line command is used to enter the Line Configuration Mode.

Example

This example shows how to enter the Line Configuration Mode for the SSH terminal line and configures its access class as "vty-filter".

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#line ssh
GA-MLxxTPoE+(config-line)#access-class vty_filter
GA-MLxxTPoE+(config-line)#
```

2.2.12 service user-account encryption

This command is used to enable the password encryption before saving in the configuration file. Use the **no** form of this command to disable the encryption.

Syntax

- **service user-account encryption**
- **no service user-account encryption**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guidelines

The information of the user account is saved in the running configuration file, and can be applied to the system later.
When this command is enabled, the password is saved in the encrypted form.
When this command is disabled and the password is specified in the plain text form, the password is saved in the plain text form. However, if the password is specified in the encrypted form or if the password has been converted to the encrypted form by the last enable password encryption command, the password will still be in the encrypted form. It cannot be reverted to the plaintext.
The password affected by this command includes the user account password and the authentication password.

Example

This example shows how to enable the password encryption function .

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#service user-account encryption
GA-MLxxTPoE+(config)#
```

2.2.13 show terminal

This command is used to obtain information about the terminal configuration parameter settings for the current terminal line. Use this command in any EXEC mode or any configuration mode.

Syntax

- **show terminal**

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guidelines

Use this command to display information about the terminal configuration parameters for the current terminal line

Example

This example shows how to display information about the terminal configuration parameter settings for the current terminal line.

```
GA-MLxxTPoE+#show terminal
 Terminal Settings:
 Length: 24 lines
 Width: 80 columns
 Default Length: 24 lines
 Default Width: 80 columns
 Baud Rate: 9600 bps

GA-MLxxTPoE+#
```

2.2.14 show users

This command is used to display information about the active lines on the Switch.

Syntax

- show users

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guidelines

This command displays information about the active lines on the Switch.

Example

This example shows how to display all session information.

```
GA-MLxxTPoE+#show users
ID   Type      User-Name       Privilege Login-Time          IP Address
--------------------------------------------------------------------------------
1    * console manager         1         4M48S

Total Entries: 1

GA-MLxxTPoE+#
```

2.2.15 telnet

This command is used to login another device that supports Telnet.

Syntax

- **telnet** [*IP-ADDRESS* | *IPV6-ADDRESS* | *Domain Name*] [*TCP-PORT*]

Parameters

Parameters	Description
IP-ADDRESS	Specifies the IPv4 address of the host.
IPV6-ADDRESS	Specifies the IPv6 address of the host.
Domain Name	Specifies the Telent destination host name.
TCP-PORT	Specifies the TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port for the Telnet protocol is 23

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guidelines

This is the Telnet client function and can be used to communicate with another device using the Telnet feature.
Multiple Telnet sessions can be opened on the Switch system and each open Telnet session can have its own Telnet client software supported at the same time

Example

This example shows how to Telnet to the IP address 10.90.90.91 using the default port 23. The IP address, 10.90.90.91 is the GA-MLxxTPoE+ management interface which allows a user to login.

```
                                GA-MLxxTPoE+


                          Product Number: PNxxxxxx
                        Firmware Version: V1.0.0.00
                             MAC Address: 00:50:40:xx:xx:xx
                           Serial Number: xxxxxxxxxxx

UserName:manager
Password:*******

GA-MLxxTPoE+#telnet 10.90.90.91
```

This example shows how to Telnet through port 23 to 10.90.90.91 and the connection failed. Try using port 3500 instead to login into the management interface.

```
                                GA-MLxxTPoE+


                          Product Number: PNxxxxxx
                        Firmware Version: V1.0.0.00
                             MAC Address: 00:50:40:xx:xx:xx
                           Serial Number: xxxxxxxxxxx

GA-MLxxTPoE+#telnet 10.90.90.91
ERROR: Could not open a connection to host on server port 23.

GA-MLxxTPoE+#telnet 10.90.90.91 3500
```

2.2.16 terminal length

The command is used to configure the number of lines displayed on the screen. The **terminal length** command will only affect the current session. The **terminal default length** command will set the default value but it does not affect the current session. The newly created, saved session terminal length will use the default value. Use the no form of this command to revert to the default setting.

Syntax

- **terminal length** *NUMBER*
- **no terminal length**
- **terminal length default** *NUMBER*
- **no terminal length default**

Parameters

Parameters	Description
NUMBER	Specifies the number of lines to display on the screen. This value must be between 0 and 512.When the terminal length is 0, the display will not stop until it reaches the end of the display.

Default

By default, this value is 24.

Command Mode

Use the User/Privileged EXEC Mode for the **terminal length** command.
Use the Global Configuration Mode for the **terminal length default** command.

Command Default Level

Level: 1 (for the **terminal length** command).
Level: 12 (for the **terminal length default** command).

Usage Guidelines

When the terminal length is 0, the display will not stop until it reaches the end of the display.

If the terminal length is specified to a value other than 0, for example 50, then the display will stop after every 50 lines. The terminal length is used to set the number of lines displayed on the current terminal screen. This command also applies to Telnet and SSH sessions. Valid entries are from 0 to 512. The default is 24 lines. A selection of 0's instructs the Switch to scroll continuously (no pausing).

Output from a single command that overflows a single display screen is followed by the **–More–** prompt. At the **–More–** prompt, press CTRL+C, q, or ESC to interrupt the output and return to the prompt. Press the Spacebar or n to display an additional screen of output, or press ENTER to display one more line of output. Setting the screen length to 0 turns off the scrolling feature and causes the entire output to display at once. Unless the **default** keyword is used, a change to the terminal length value applies only to the current session. When using the no form of this command, the number of lines in the terminal display screen is reset to 24.
The **terminal length default** command is available in the global configuration mode. The command setting does not affect the current existing terminal sessions but affects the new terminal sessions that are activated later. Only the default terminal length value can be saved.

Example

This example shows how to change the lines to be displayed on a screen to 60.

```
GA-MLxxTPoE+#terminal length 60
GA-MLxxTPoE+#
```

2.2.17 terminal speed

This command is used to setup the terminal speed. Use the **no** form of this command to revert to the default setting.

Syntax

- **terminal speed** *BPS*
- **no terminal speed**

Parameters

Parameters	Description
BPS	Specifies the console rate in bits per second (bps). Valid values are 9600, 38400, 19200, 115200

Default

By default, this value is 9600.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use this command to configure the terminal connection speed. Some baud rates available on the devices connected to the port might not be supported on the Switch.

Example

This example shows how to configure the serial port baud rate to 9600 bps.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#terminal speed 9600
GA-MLxxTPoE+(config)#
```

2.2.18 session timeout

This command is used to configure the line session timeout value. Use the **no** form of this command to revert to the default setting.

Syntax

- **session-timeout** *MINUTES*
- **no session-timeout**

Parameters

Parameters	Description
MINUTES	Specifies the timeout length in minutes. 0 represents never timeout.

Default

By default, this value is 3 minutes.

Command Mode

Line Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

This timer specifies the timeout for auto-logout sessions established by the line that is being configured.

Example

This example shows how to configure the console session to never timeout.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#line console
GA-MLxxTPoE+(config-line)#session-timeout 0
GA-MLxxTPoE+(config-line)#
```

2.2.19 username

This command is used to create a user account. Use the **no** command to delete the user account.

Syntax

- **username** *NAME* [**privilege** *LEVEL*] [**nopassword** | **password** [**0** | **7**] *PASSWORD*]
- **no username** [*NAME*]

Parameters

Parameters	Description
NAME	Specifies the user name with a maximum of 32 characters.
privilege *LEVEL*	(Optional) Specifies the privilege level for each user. The privilege level must be between 1 and 15.
nopassword	(Optional) Specifies that there will be no password associated with this account.
password	(Optional) Specifies the password for the user.

Parameters	Description
0	(Optional) Specifies the password in clear, plain text. The password length is between 1 and 32 characters and can contain embedded spaces. It is case-sensitive. If the password syntax cannot be specified, the syntax remains plain text.
7	(Optional) Specifies the encrypted password based on SHA-1. The password length is fixed at 35 bytes. It is case-sensitive. The password is encrypted. If the password syntax is not specified, the syntax is plain text.
PASSWORD	(Optional) Specifies the password string based on the type.

Default

By default, no username-based authentication system is established.
If not specified, use 1.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guidelines

This command creates user accounts with different access levels. When the user login with Level 1, the user will be in the User EXEC Mode. The user needs to further use the **enable** command to enter the Privileged EXEC Mode.
When the user login with a Level higher than or equal to 2, the user will directly enter the Privileged EXEC Mode. Therefore, the Privileged EXEC Mode can be in Levels 2 to 15.
The user can specify the password in the encrypted form or in the plain-text form. If it is in the plain-text form, but the service password encryption is enabled, then the password will be converted to the encrypted form.
If the **no username** command is used without the user name specified, all users are removed.
By default, the user account is empty. When the user account is empty, the user will be directly in the User EXEC Mode at Level 1. The user can further enter the Privileged EXEC Mode using the **enable** command.

Example

This example shows how to create an administrative username, called **admin**, and a password, called “mypassword”.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#username admin privilege 15 password 0 mypassword
GA-MLxxTPoE+(config)#
```

This example shows how to remove the user account with the username **admin**.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#no username admin
GA-MLxxTPoE+(config)#
```

2.2.20 password

This command is used to create a new password. Use the **no** form of this command to remove the password.

Syntax

- **password** [0 | 7] *PASSWORD*
- **no password**

Parameters

Parameters	Description
0	(Optional) Specifies the password in clear, plain text. The password length is between 1 and 32 characters and can contain embedded spaces. It is case-sensitive. If the password syntax cannot be specified, the syntax remains plain text.
7	(Optional) Specifies the encrypted password based on SHA-1. The password length is fixed at 35 bytes. It is case-sensitive. The password is encrypted. If the password syntax is not specified, the syntax is plain text.
PASSWORD	Specifies the password for the user.

Default

None

Command Mode

Line Configuration Mode

Command Default Level

Level: 15

Usage Guidelines

This command is used to create a new user password. Only one password can be used for each type of line.

Example

This example shows how to create a password for the console line.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#line console
GA-MLxxTPoE+(config-line)#password 123
GA-MLxxTPoE+(config-line)#
```

2.2.21 clear line

This command is used to disconnect a connection session.

Syntax

- **clear line** *LINE-ID*

Parameters

Parameters	Description
LINE-ID	Specifies the line ID of the connection session that will be disconnected.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 15

Usage Guidelines

Use this command to disconnect an active session on the Switch. The line ID is assigned by line when the connection session was created. Use the **show users** command to view active sessions.
This command can only disconnect SSH and Telnet sessions.

Example

This example shows how to disconnect the line session 1.

```
GA-MLxxTPoE+#clear line 1
GA-MLxxTPoE+#
```

2.2.22 do

This command is used to execute commands orgininally in the User/Privileged EXEC mode in the global configuration mode or other configuration modes.

Syntax

- **do** *COMMAND*

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use this command to execute commands orgininally in the User/Privileged EXEC mode, such as **show**, **clear**, or **debug**, while configuring your routing device. After the command is executed, the system will return to the configuration mode you were using.

Example

This example shows how to execute the show running-config command in the global configuration mode.

```
                                    GA-MLxxTPoE+


                                  Product Number: PNxxxxxx
                                Firmware Version: V1.0.0.00
                                     MAC Address: 00:50:40:xx:xx:xx
                                   Serial Number: xxxxxxxxxxx


UserName:manager
Password:*******

GA-MLxxTPoE+>enable
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#do show running-config
Building configuration...

Current configuration : 961 bytes

!-------------------------------------------------------------------------------
!                        GA-ML8TPoE+ Gigabit Ethernet Switch
!                                  Configuration
!
!                              Firmware: Build V1.0.0.00
!                Copyright(C) 2019 Panasonic. All rights reserved.
!-------------------------------------------------------------------------------

enable
config
!
spanning-tree mst configuration
 exit
!
line console
 exit
!
line ssh
 exit
--More--
```

2.3 SSH (Secure Shell) Commands

2.3.1 crypto key generate

This command is used to generate the RSA or DSA key pair.

Syntax

- **crypto key generate {rsa [modulus** *MODULUS-SIZE*] | **dsa}**

Parameters

Parameters	Description
rsa	Specifies to generate the RSA key pair.
modulus *MODULUS-SIZE*	(Optional) Specifies the number of bits in the modulus. For RSA, the valid values are 360, 512, 768, 1024, and 2048.If not specified, a message will be promoted to the user to specify the value.
dsa	Specifies to generate the DSA key pair. The DSA key size is fixed as 1024 bit.

Default

Key pair is assigned by default.

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 15

Usage Guideline

This command is used to generate the RSA or DSA key pair.

Example

This example shows how to create an RSA key.

```
GA-MLxxTPoE+#crypto key generate rsa

Choose the size of the key modulus in the range of 360 to 2048. The process may
take a few minutes.
Number of bits in the modulus [768]: 768
Generating RSA key...Done.

GA-MLxxTPoE+#
```

2.3.2 crypto key zeroize

This command is used to delete the RSA or DSA key pair.

Syntax

- **crypto key zeroize {rsa | dsa}**

Parameters

Parameters	Description
rsa	Specifies to delete the RSA key pair.
dsa	Specifies to delete the DSA key pair.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 15

Usage Guideline

This command deletes the public key pair of the SSH Server. If both RSA and DSA key pairs are deleted, the SSH server will not be in service.

Example

This example shows how to delete the RSA key.

```
GA-MLxxTPoE+#crypto key zeroize rsa

Do you really want to remove the key? (y/n)[n]: y

GA-MLxxTPoE+#
```

2.3.3 ip ssh timeout

This command is used to configure the SSH control parameters on the Switch. Use the **no** form of this command to revert to the default setting.

Syntax

- **ip ssh** {**timeout** *SECONDS* | **authentication-retries** *NUMBER*}
- **no ip ssh** {**timeout** | **authentication-retries**}

Parameters

Parameters	Description
timeout *SECONDS*	Specifies the time interval that the Switch waits for the SSH client to respond during the SSH negotiation phase. The range is from 30 to 600.
authentication-retries *NUMBER*	Specifies the number of authentication retry attempts. The session is closed if all the attempts fail. The range is from 1 to 32.

Default

By default, the timeout value is 120 seconds.
By default, the authentication retries is 3.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to configure the SSH server parameters on the Switch. The authentication retry number specifies the maximum number of retry attempts before the session is closed.

Example

This example shows how to configure the SSH timeout value to 160 seconds.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#ip ssh timeout 160
GA-MLxxTPoE+(config)#
```

This example shows how to configure the SSH authentication retries value to 2 times. The connection fails after 2 retry attempt fails.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#ip ssh authentication-retries 2
GA-MLxxTPoE+(config)#
```

2.3.4 ip ssh server

This command is used to enable the SSH server function. Use the **no** form of this command to disable the SSH server function.

Syntax

- **ip ssh server**
- **no ip ssh server**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to enable the SSH server function. After enabling the SSH server, you can log-in within the range of the user-mode.

Example

This example shows how to enable the SSH server function.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#ip ssh server
GA-MLxxTPoE+(config)#
```

2.3.5 ip ssh service-port

This command is used to specify the service port for SSH. Use the **no** form of this command to revert to the default setting.

Syntax

- **ip ssh service-port** *TCP-PORT*
- **no ip ssh service-port**

Parameters

Parameters	Description
TCP-PORT	Specifies the TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port for the SSH protocol is 22.

Default

By default, this value is 22.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command configures the TCP port number for SSH server.

Example

This example shows how to change the service port number to 3000.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#ip ssh service-port 3000
GA-MLxxTPoE+(config)#
```

2.3.6 show crypto key mypubkey

This command is used to display the RSA or DSA public key pairs.

Syntax

- **show crypto key mypubkey {rsa | dsa}**

Parameters

Parameters	Description
rsa	Specifies to display information regarding the RSA public key.
dsa	Specifies to display information regarding the DSA public key.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to display the RSA or DSA public key pairs.

Example

This example shows how to display the information regarding the RSA public key.

```
GA-MLxxTPoE+#show crypto key mypubkey rsa

% Key pair was generated at: 09:48:40, 2013-11-29
Key Size: 768 bits
Key Data:
AAAAB3Nz aC1yc2EA AAADAQAB AAAAQwCN 6IRFHCBf jsHvYjQG iCL0p2kz 2v38ULC8
kAKra/Ze mG7IW3eC 8STcrkr5 s7l9H/bh jG/oqkwj SlUJSGqR e/sj6Ws=

GA-MLxxTPoE+#
```

2.3.7 show ip ssh

This command is used to display the user SSH configuration settings.

Syntax

- show ip ssh

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to the SSH configuration settings.

Example

This example shows how to display the SSH configuration settings.

```
GA-MLxxTPoE+#show ip ssh

IP SSH server              : Enabled
IP SSH service port        : 22
SSH server mode            : V2
Authentication timeout     : 120 secs
Authentication retries     : 3 times

GA-MLxxTPoE+#
```

2.3.8 show ssh

This command is used to display the status of SSH server connections.

Syntax

- **show ssh**

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display the SSH connections' status on the Switch.

Example

This example shows how to display SSH connections' information.

```
GA-MLxxTPoE+#show ssh

SID Ver. Cipher                       Userid           Client IP Address
--- --- ---------------------------- ---------------- ------------------------
0   V2  3des-cbc/sha1-96             zhang3           192.168.0.100
1   V2  3des-cbc/hmac-sha1           lee4567890123456 2000::243

Total Entries: 2

GA-MLxxTPoE+#
```

Display Parameters

Parameters	Description
SID	A unique number that identifies the SSH session.
Ver	Indicates the SSH version of this session.
Cipher	The cryptographic / Hashed Message Authentication Code (HMAC) algorithm that the SSH client is using.
Userid	The login username of the session.
Client IP Address	The client IP address for this established SSH session.

2.3.9 ssh user authentication-method

This command is used to configure the SSH authentication method for a user account. Use the **no** form of this command to revert to the default settings.

Syntax

- **ssh user** *NAME* **authentication-method {password | publickey** *URL* **| hostbased** *URL* **host-name** *HOSTNAME* **[***IP-ADDRESS* **|** *IPV6-ADDRESS***]}**
- **no ssh user** *NAME* **authentication-method**

Parameters

Parameters	Description
NAME	Specifies the username to configure the authentication type. The user must be an existing local account. The length of the username is limited to a maximum of 32 characters.
password	Specifies to use the password authentication method for this user account. This is the default authentication method.

Parameters	Description
publickey *URL*	Specifies to use the public key authentication method for this user account. Enter the URL of a local file to be used as the public key of this user.
hostbased *URL*	Specifies to use the host-based authentication method for this user account. Enter the URL of a local file to be used as client's host key.
host-name *HOSTNAME*	Specifies the allowed host name for host-based authentication. During authentication phase, the client's hostname will be checked. The range is from 1 to 255.
IP-ADDRESS	(Optional) Specifies whether to additionally check the IP address of the client for host-based authentication. If not specified, only the host name will be checked.
IPV6-ADDRESS	(Optional) Specifies whether to additionally check the IPv6 address of the client for host-based authentication. If not specified, only the host name will be checked.

Default

The default authentication method for a user is password.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

The administrator can use this command to specify authentication method for a user. The user name must be a user created by the **username** command. By default, the authentication method is password. The system will prompt the user to input the password.
To authenticate a user via SSH public key authentication, copy the user's public key file to file system. When the user tries to log into the Switch via an SSH client (using the SSH public key method), the SSH client will automatically transmit the public key and signature with the private key to the Switch. If both the public key and signature are correct, the user is authenticated and login into the Switch is allowed.

- To authenticate a user via SSH public key authentication via SSH public key or the host-based method, the user's public key file or client's host key file must be specified. Both key files have the same format. A key file can contain multiple keys and each key is defined by one line. The maximum length of one line is 8 Kb.
- Each key consists of the following space-separated fields: *keytype*, *base64-encoded key*, and *comment*. The *keytype* and *base64-encoded key* fields are mandatory and the *comment* field is optional. The *keytype* field can be either be *ssh-dss* or *ssh-rsa*.

Example

This example shows how to configure the authentication method to public key for user user1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#ssh user user1 authentication-method publickey c:/user1.pub
GA-MLxxTPoE+(config)#
```

2.4 IP Utility Commands

2.4.1 ping

This command is used to diagnose basic network connectivity.

Syntax

- **ping** {[**ip**] *IP-ADDRESS* | [**ipv6**] *IPV6-ADDRESS* | *HOST-NAME*} [**count** *TIMES*] [**timeout** *SECONDS*]

Parameters

Parameters	Description
ip	(Optional) Specifies to use the IPv4 address.
IP-ADDRESS	Specifies the IPv4 address of the destination host.
ipv6	(Optional) Specifies to use the IPv6 address.
IPV6-ADDRESS	Specifies the IPv6 address of the system to discover.
HOST-NAME	Specifies the host name of the system to discover.
count *TIMES*	(Optional) Specifies to stop after sending the specified number of echo request packets.
timeout *SECONDS*	(Optional) Specifies response timeout value, in seconds.
frequency *SECONDS*	(Optional) Specifies the frequency time for ping.

Default

The **count** value is disabled. The ping will continue until the user terminates the process.
The **timeout** value is 1 second.

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guidelines

Use this command to verify the reachability, reliability, and delay of the path to the destination host. If neither the **count** or **timeout** value is specified, the only way to stop the ping is by pressing Ctrl-C.

Example

This example shows how to ping the host with IP address 172.50.71.123.

```
GA-MLxxTPoE+#ping 172.50.71.123 count 5

Reply from 172.50.71.123, time<10ms
Reply from 172.50.71.123, time<10ms
Reply from 172.50.71.123, time<10ms
Reply from 172.50.71.123, time<10ms
Reply from 172.50.71.123, time<10ms

 Ping Statistics for 172.50.71.123
 Packets: Sent =5, Received =5, Lost =0

GA-MLxxTPoE+#
```

This example shows how to ping the host with IPv6 address 2001:238:f8a:77:7c10:41c0:6ddd:ecab.

```
GA-MLxxTPoE+#ping 2001:238:f8a:77:7c10:41c0:6ddd:ecab count 3

Reply from 2001:238:f8a:77:7c10:41c0:6ddd:ecab, bytes=100, time<10 ms
Reply from 2001:238:f8a:77:7c10:41c0:6ddd:ecab, bytes=100, time<10 ms
Reply from 2001:238:f8a:77:7c10:41c0:6ddd:ecab, bytes=100, time<10 ms

 Ping Statistics for 2001:238:F8A:77:7C10:41C0:6DDD:EACB
 Packets: Sent =3, Received =3, Lost =0

GA-MLxxTPoE+#
```

2.4.2 ping access-class

This command is used to specify an access list to restrict the access via ping. Use the **no** form of this command to remove the access list check.

Syntax

- **ping access-class** *IP-ACL*
- **no ping access-class**

Parameters

Parameters	Description
IP-ACL	Specifies a standard IP access list. The source address field of the permit or deny entry defines the valid or invalid host.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

This command specifies an access list to restrict the access via ping.

Example

This example shows how a standard IP access list is created and is specified as the access list to restrict access via ping. Only the host 226.1.1.1 is allowed to ping the Switch.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip access-list ping-filter
GA-MLxxTPoE+(config-ip-acl)# permit 226.1.1.1 0.0.0.0
GA-MLxxTPoE+(config-ip-acl)# exit
GA-MLxxTPoE+(config)# ping access-class ping-filter
GA-MLxxTPoE+(config)#
```

2.4.3 traceroute

This command is used to display a hop-by-hop path from the Switch through an IP network to a specific destination host.

Syntax

- **traceroute** {[**ip**] *IP-ADDRESS* | [**ipv6**] *IPV6-ADDRESS* | *HOST-NAME*} [**probe** *NUMBER*] [**timeout** *SECONDS*] [**max-ttl** *TTL*] [**port** *DEST-PORT*]

Parameters

Parameters	Description
ip	(Optional) Specifies to use the IPv4 address.
IP-ADDRESS	Specifies the IPv4 address of the destination host.
ipv6	(Optional) Specifies to use the IPv6 address.
IPV6-ADDRESS	Specifies the IPv6 address of the system to discover.
HOST-NAME	Specifies the host name of the system to discover.
probe *NUMBER*	(Optional) Specifies the number of datagrams to send. The allowed range is from 1 to 1000.
timeout *SECONDS*	(Optional) Specifies the response timeout value, in seconds.
max-ttl *TTL*	(Optional) Specifies the maximum TTL value for outgoing UDP datagrams. The maximum allowed range is from 1 to 255.
port *DEST-PORT*	(Optional) Specifies the base UDP destination port number used in outgoing datagrams. This value is incremented each time a datagram is sent. The allowed range for the destination port is from 1 to 65535. Use this option in the unlikely event that the destination host is listening to a port in the default trace-route port range.

Default

The maximum TTL value is 30.
The timeout period is 5 seconds.
The destination base UDP port number is 33434.
The query number for each TTL is 3.

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guidelines

To interrupt this command after the command has been issued, press Ctrl-C.

This command uses the TTL field in the IP header to cause routers and servers to generate specific return messages. A **traceroute** starts by sending a UDP datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends back an ICMP time-exceeded message to the sender. The **traceroute** facility determines the address of the first hop by examining the source address field of the ICMP time-exceeded message. To identify the next hop, **traceroute** again sends a UDP packet, but this time with a TTL value of 2. The first router decrements the TTL field by 1 and send the datagram to the next router. The second router sees a TTL value of 1, discards the datagram, and returns the time-exceeded message to the source. This process continues until the TTL is incremented to a value large enough for the datagram to reach the destination host (or until the maximum TTL is reached). To determine when a datagram has reached its destination, **traceroute** sets the UDP destination port in the datagram to a very large value that the destination host is unlikely to be using. When a host receives a datagram with an unrecognized port number, it sends an ICMP port unreachable error to the source. This message indicates to the **traceroute** facility that it has reached the destination.

Example

This example shows how to trace-route the host 172.50.71.123.

```
GA-MLxxTPoE+# traceroute 172.50.71.123

<10 ms  172.50.71.123

Trace complete.
GA-MLxxTPoE+#
```

This example shows how to trace-route to the host 172.50.71.123, but the router does not reply.

```
GA-MLxxTPoE+# traceroute 172.50.71.123

  *      Request timed out.
  *      Request timed out.
GA-MLxxTPoE+#
```

This example shows how to trace-route to the host 172.50.71.123, but the router replies that the destination is unreachable.

```
GA-MLxxTPoE+# traceroute 172.50.71.123

<10 ms  Network Unreachable

GA-MLxxTPoE+#
```

This example shows how to trace-route to the host with the IPv6 address 2001:238:f8a:77:7c10:41c0:6ddd:ecab.

```
GA-MLxxTPoE+# traceroute 2001:238:f8a:77:7c10:41c0:6ddd:ecab
<10 ms  2001:238:f8a:77:7c10:41c0:6ddd:ecab

Trace complete.
GA-MLxxTPoE+#
```

2.5 File System Commands

2.5.1 cd

This command is used to change the current directory.

Syntax

- **cd** [*DIRECTORY-URL*]

Parameters

Parameters	Description
DIRECTORY-URL	(Optional) Specifies the URL of the directory. If not specified, the current directory will be shown.

Default

The default current directory is the root directory on the file system of the local FLASH.

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

If the URL is not specified, then the current directory is not changed.

Example

This example shows how to change the current directory to the directory “d” on file system.

```
GA-MLxxTPoE+#dir

Directory of /c:
1    -rw      12785484 Jan 15 2017 01:41:56  runtime.had
2    -rw         35856 Jan 20 2017 04:58:06  config.cfg
3    -rw      12799156 Jan 20 2017 04:57:18  firmware.had
4    -rw      12481700 Jan 15 2017 23:57:11  fw5.had
5    -rw      12791928 Jan 05 2017 23:09:30  backup.had
6    d--             0 Jan 23 2017 03:49:07  system

125304832 bytes total (70426624 bytes free)

GA-MLxxTPoE+#cd d:
GA-MLxxTPoE+#
```

This example shows how to display the current directory.

```
GA-MLxxTPoE+#cd
Current directory is /c:
GA-MLxxTPoE+#
```

2.5.2 delete

This command is used to delete a file.

Syntax

- **delete** *FILE-URL*

Parameters

Parameters	Description
FILE-URL	Specifies the name of the file to be deleted.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 15

Usage Guideline

The firmware image or the configuration file that is specified as the boot-up file cannot be deleted.

Example

This example shows how to delete the file named “test.txt” from file system on the local flash.

```
GA-MLxxTPoE+# delete test.txt

Delete test.txt? (y/n) [n] y
File is deleted

GA-MLxxTPoE+#
```

2.5.3 dir

This command is used to display the information for a file or the listing of files in the specified path name.

Syntax

- **dir** [*URL*]

Parameters

Parameters	Description
URL	(Optional) Specifies the name of the file or directory to be displayed.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

If URL is not specified, the current directory is used. By default, the current directory is located at the root of the file system located at local flash. The storage media is mounted in the file system and appears to the user as a sub-directory under the root directory.
The supported file systems can be displayed as the user issues the **dir** command for the root directory. The storage media that is mapped to the file system can be displayed by using the **show storage media** command.

Example

This example shows how to display the root directory in a standalone switch.

```
GA-MLxxTPoE+#dir /

Directory of /
1    d--              0 Jan 23 2017 03:49:07   c:

0 bytes total (0 bytes free)

GA-MLxxTPoE+#
```

2.5.4 mkdir

This command is used to create a directory under the current directory.

Syntax

- **mkdir** *DIRECTORY-NAME*

Parameters

Parameters	Description
DIRECTORY-NAME	Specifies the name of the directory.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to make a directory in the current directory.

Example

This example shows how to create a directory named “newdir” under the current directory.

```
GA-MLxxTPoE+# mkdir newdir
GA-MLxxTPoE+#
```

2.5.5 rename

This command is used to rename a file.

Syntax

- **rename** *FILE-PATH1 FILE-PATH2*

Parameters

Parameters	Description
FILE-PATH1	Specifies the path for the file to be renamed.
FILE-PATH2	Specifies the path after file renaming.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 15

Usage Guideline

A file can be renamed to a file located either within the same directory or to another directory.

Example

This example shows how to rename file called “doc.1” to “test.txt”.

```
GA-MLxxTPoE+# rename doc.1 test.txt

Rename file doc.1 to text.txt? (y/n) [n] y

GA-MLxxTPoE+#
```

2.5.6 rmdir

This command is used to remove a directory in the file system.

Syntax

- **rmdir** *DIRECTORY-NAME*

Parameters

Parameters	Description
DIRECTORY-NAME	Specifies the name of the directory.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to remove a directory in the working directory.

Example

This example shows how to remove a directory called “newdir” under the current directory.

```
GA-MLxxTPoE+# rmdir newdir

Remove directory newdir? (y/n) [n] y
The directory is removed

GA-MLxxTPoE+#
```

2.5.7 show storage media-info

This command is used to display the storage media’s information.

Syntax

- **show storage media-info**

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display the information of the storage media available on the system.

Example

This example shows how to display the information of the storage media on all units.

```
GA-MLxxTPoE+#show storage media-info

Unit  Drive  Media-Type  Size     FS-Type   Label
----  -----  ----------  -------  --------  -------------
 1    c:     FLASH       100M     UBIS

GA-MLxxTPoE+#
```

Display Parameters

Parameters	Description
Media-Type	**FLASH:** This represents the storage in the Switch. **SD Card:** This represents removable storage devices.

2.6 System Log Commands

2.6.1 clear logging

This command is used to delete log messages in the system logging buffer.

Syntax

- clear logging

Parameters

None

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

This command deletes all the log messages in the system logging buffer.

Example

This example shows how to delete all the log messages in the logging buffer.

```
GA-MLxxTPoE+# clear logging
Clear logging? (y/n) [n] y
GA-MLxxTPoE+#
```

2.6.2 logging on

This command is used to enable the logging of system messages. Use the no form of this command to disable the logging of system messages.

Syntax

- logging on
- no logging on

Parameters

None

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

To enable the logging of system messages, use the **logging on** command in the global configuration mode. This command sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages. To disable the logging process, use the **no** form of this command.
The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, terminal lines, or the syslog server. System logging messages are also known as system error messages. Logging can be turned on and off for these destinations individually using the **logging buffered**, **logging server**, and logging global configuration commands. However, if the **logging on** command is disabled, no messages will be sent to these destinations. If the **logging on** command is enabled, the logging buffered will be enabled at the same time.

Example

This example shows how to enable the logging of system messages.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# logging on
WARNING: The command takes effect and the logging buffered is enabled at the same
time.
GA-MLxxTPoE+(config)#
```

2.6.3 logging buffered

This command is used to enable logging of system messages to the local message buffer. Use the **no** form of this command to disable the logging of messages to the local message buffer. Use the **default logging buffered** command to revert to default setting.

Syntax

- **logging buffered** [**severity** {*SEVERITY-LEVEL* | *SEVERITY-NAME*}] [**discriminator** *NAME*] [**write-delay** {*SECONDS* | **infinite**}]
- **no logging buffered**
- **default logging buffered**

Parameters

Parameters	Description
SEVERITY-LEVEL	(Optional) Specifies the severity level of system messages. The messages at that severity level or a more severe level will be logged to message buffers. This value must be between 0 and 7. 0 is the most severe level. The corresponding severity levels are listed together with their respective severity names: emergencies (**0**), alerts (**1**), critical (**2**), errors (**3**), warnings (**4**), notifications (**5**), informational (**6**), debugging (**7**). If not specified, the default severity level is warnings (**4**).
SEVERITY-NAME	(Optional) Specifies the severity level name of system messages. The corresponding severity levels are listed together with their respective severity names: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7).
discriminator	(Optional) Specifies to filter the message to be sent to local buffer based on the discriminator.
write-delay *SECONDS*	(Optional) Specifies to delay periodical writing of the logging buffer to the FLASH by the amount of seconds specified.

Default

By default, the severity level is warning (4).

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The system messages can be logged to the local message buffer or to other destinations. Messages must enter the local message buffer first before it can be further dispatched to other destinations.
This command does not take effect if the specified discriminator does not exist. Thus the default setting of the command is applied.
Specify the severity level of the messages in order to restrict the system messages that are logged in the logging buffer (thus reducing the number of messages logged). The messages which are at the specified severity level or higher will be logged to the message buffer. When the logging buffer is full, the oldest log entries will be removed to create the space needed for the new messages that are logged.
The content of the logging buffer will be saved to the FLASH memory periodically such that the message can be restored on reboot. The interval for periodically writing the logging buffer to FLASH can be specified. The content of the logged messages in the FLASH will be reloaded into the logging buffer on reboot.

Example

This example shows how to enable the logging of messages to the logging buffer and restrict logging of messages with a security level of errors or higher.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# logging buffered severity errors
GA-MLxxTPoE+(config)#
```

2.6.4 logging console

This command is used to enable the logging of system messages to the local console. Use the **no** form of this command to disable the logging of messages to the local console and revert to the default setting.

Syntax

- **logging console [severity {***SEVERITY-LEVEL* | *SEVERITY-NAME*}] [discriminator *NAME*]
- **no logging console**

Parameters

Parameters	Description
SEVERITY-LEVEL	(Optional) Specifies the severity level of system messages. The messages at that severity level or a more severe level will be logged to message buffers. This value must be between 0 and 7. 0 is the most severe level. The corresponding severity levels are listed together with their respective severity names: emergencies (**0**), alerts (**1**), critical (**2**), errors (**3**), warnings (**4**), notifications (**5**), informational (**6**), debugging (**7**). If not specified, the default severity level is warnings (**4**).
SEVERITY-NAME	(Optional) Specifies the severity level name of system messages. The corresponding severity levels are listed together with their respective severity names: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7).
discriminator	(Optional) Specifies to filter the message to be sent to the local console based on the discriminator.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The system messages can be logged to the local message buffer, local console or other destinations. Messages must enter the local message buffer first before it can further be dispatched to the console.
This command does not take effect if the specified discriminator does not exist. Thus the default setting of the command is applied.
Specify the severity level of the messages in order to restrict the system messages that are logged to the console. The messages which are at the specified severity level or higher will be dispatched to the local console.

Example

This example shows how to enable the logging of messages to the local console and restrict the logging of messages with a security level of errors or higher.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# logging console severity errors
GA-MLxxTPoE+(config)#
```

2.6.5 logging discriminator

This command is used to create a discriminator that can be further used to filter SYSLOG messages sent to various destinations.

Syntax

- **logging discriminator** *NAME* [**facility** {**drops** *STRING* | **includes** *STRING*}] [**severity** {**drops** *SEVERITY-LIST* | **includes** *SEVERITY-LIST*}]
- **no discriminator** *NAME*

Parameters

Parameters	Description
NAME	Specifies the name of the discriminator.
facility	(Optional) Specifies a sub-filter based on the facility string.
STRING	Specifies one or more facility names. If multiple facility names are used, they should be separated by commas without spaces before and after the comma.
includes	Specifies to include the matching message. The unmatched messages are filtered.
drops	Specifies to filter the matching message.
severity	(Optional) Specifies a sub-filter based on severity matching.
SEVERITY-LIST	Specifies a list of severity levels to be filtered or to be included.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

An existing discriminator can be configured. The later setting will overwrite the previous setting. Associate a discriminator with the logging buffered and the logging server command.

Example

This example shows how to create a discriminator named “buffer-filter” which specifies two sub-filters, one based on the severity level and the other based on the facility.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# logging discriminator buffer-filter facility includes STP
severity includes 1-4,6
GA-MLxxTPoE+(config)#
```

2.6.6 logging server

This command is used to create a SYSLOG server host to log the system messages or debug output. Use the **no** command to remove a SYSLOG server host.

Syntax

- **logging server** {*IP-ADDRESS* | *IPV6-ADDRESS*} [**severity** {*SEVERITY-LEVEL* | *SEVERITY-NAME*}] [**facility** {*FACILITY-NUM* | *FACILITY-NAME*}] [**discriminator** *NAME*] [**port** *UDP-PORT*]
- **no logging server** {*IP-ADDRESS* | *IPV6-ADDRESS*}

Parameters

Parameters	Description
IP-ADDRESS	Specifies the IP address of the SYSLOG server host.
IPV6-ADDRESS	Specifies the IPv6 address of the log server host.

Parameters	Description
SEVERITY-LEVEL	(Optional) Specifies the severity level of system messages. The messages at that severity level or a more severe level will be logged to message buffers. This value must be between 0 and 7. 0 is the most severe level. The corresponding severity levels are listed together with their respective severity names: emergencies (**0**), alerts (**1**), critical (**2**), errors (**3**), warnings (**4**), notifications (**5**), informational (**6**), debugging (**7**). If not specified, the default severity level is warnings (**4**).
SEVERITY-NAME	(Optional) Specifies the severity level name of system messages. The corresponding severity levels are listed together with their respective severity names: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7).
FACILITY-NUM	(Optional) Specifies a decimal value from 0 to 23 to represent the facility. If not specified, the default facility is local7 (**23**). See the usage guideline for more information.
FACILITY-NAME	(Optional) Specifies a facility name to represent the facility. If not specified, the default facility is **local7** (23). See the usage guideline for more information.
discriminator *NAME*	(Optional) Specifies to filter the message to the log server based on discriminator.
port *UDP-PORT*	(Optional) Specifies the UDP port number to be used for the SYSLOG server. Valid values are 514 (the IANA well-known port) or any value from 1024 to 65535. If not specified, the default UDP port is 514.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

System messages can be logged to the local message buffer, local console or remote hosts. Messages must enter the local message buffer first before it can be further dispatched to logging server.

The following is a table for the facility.

Facility Number	Facility Name	Facility Description
0	kern	Kernel messages.
1	user	User-level messages.
2	mail	Mail system.
3	daemon	System daemons.
4	auth1	Security/authorization messages.
5	syslog	Messages generated internally by the SYSLOG.
6	lpr	Line printer sub-system.
7	news	Network news sub-system.
8	uucp	UUCP sub-system.
9	clock1	Clock daemon.
10	auth2	Security/authorization messages.
11	ftp	FTP daemon.
12	ntp	NTP subsystem.
13	logaudit	Log audit.
14	logalert	Log alert.
15	clock2	Clock daemon (note 2).
16	local0	Local use 0 (local0).
17	local1	Local use 1 (local1).
18	local2	Local use 2 (local2).
19	local3	Local use 3 (local3).
20	local4	Local use 4 (local4).
21	local5	Local use 5 (local5).
22	local6	Local use 6 (local6).
23	local7	Local use 7 (local7).

Example

This example shows how to enable the logging of system messages with a severity higher than warnings to the remote host 20.3.3.3.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# logging server 20.3.3.3 severity warnings
GA-MLxxTPoE+(config)#
```

2.6.7 logging smtp

This command is used to enable the logging of system messages to email recipients. Use the **no** command to disable the logging of messages to email recipients and revert to the default setting.

Syntax

- **logging smtp [severity** {*SEVERITY-LEVEL* | *SEVERITY-NAME*}] **[discriminator** *NAME*]
- **no logging smtp**

Parameters

Parameters	Description
SEVERITY-LEVEL	(Optional) Specifies the severity level of system messages. The messages at that severity level or a more severe level will be logged to message buffers. This value must be between 0 and 7. 0 is the most severe level. The corresponding severity levels are listed together with their respective severity names: emergencies (**0**), alerts (**1**), critical (**2**), errors (**3**), warnings (**4**), notifications (**5**), informational (**6**), debugging (**7**). If not specified, the default severity level is warnings (**4**).
SEVERITY-NAME	(Optional) Specifies the severity level name of system messages. The corresponding severity levels are listed together with their respective severity names: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7).
discriminator *NAME*	(Optional) Specifies to filter the message to email recipients based on the discriminator.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The system messages can also be logged to email recipients. This command does not take effect if the specified discriminator does not exist. Thus the default setting of the command is applied. Messages must enter the local message buffer first before it can be further dispatched to email recipients.
Specify the severity level of the messages in order to restrict the system messages that are logged. The messages which are at the specified severity level or higher will be logged to the email recipients.

Example

This example shows how to enable the logging of system messages with a severity higher than warnings to email recipients.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# logging smtp severity warnings
GA-MLxxTPoE+(config)#
```

2.6.8 show logging

This command is used to display the system messages logged in the local message buffer.

Syntax

- **show logging** [**all** | [*REF-SEQ*] [**+** *NN* | **-** *NN*]]

Parameters

Parameters	Description
all	(Optional) Specifies to display all log entries starting from the latest message.
REF-SEQ	(Optional) Specifies to start the display from the reference sequence number.
+ *NN*	(Optional) Specifies the number of messages that occurred after the specified reference sequence number. If the reference index is not specified, it starts from the eldest message in the buffer.
- *NN*	(Optional) Specifies the number of messages that occurred prior to the specified reference sequence number. If the reference index is not specified, the message display starts from the last message written in the buffer.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display the system messages logged in the local message buffer.
Each message logged in the message buffer is associated with a sequence number. As a message is logged, a sequence number starting from 1 is allocated. The sequence number will roll back to 1 when it reaches 100000.
When the user specifies to display a number of messages following the reference sequence number, the oldest messages are displayed prior to the newer messages. When the user specifies to display a number of messages prior to the reference sequence number, the newer messages are displayed prior to the later messages.
If the command is issued without options, the system will display up to 200 entries starting from the latest message.

Example

This example shows how to display the messages in the local message buffer.

```
GA-MLxxTPoE+# show logging

Total number of buffered messages: 2
#2 2017-03-25 16:37:36 Unit 1, Successful login through Console (Username: Anonymous)
#1 2017-03-25 16:35:54 INFO(6) Port Gi1/0/1 link up, 1000Mbps FULL duplex

GA-MLxxTPoE+#
```

2.6.9 show attack-logging

This command is used to display attack log messages.

Syntax

- **show attack-logging [index** *INDEX*]

Parameters

Parameters	Description
index *INDEX*	Specifies the list of index numbers of the entries that need to be displayed. If no index is specified, all entries in the attack log DB will be displayed.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display the attack log messages. The attack log message refers to log messages driven by modules such as DOS and the port-security module. This type of log message may generate a large amount of messages and quickly cause the system to run out of system log storage. Therefore, for this type of log messages only the first log that is generated each minute can be stored in the system log, with the rest of them being stored in a separate table named attack log.

Example

This example shows how to display the first attack log entry.

```
GA-MLxxTPoE+# show attack-logging
Attack log messages:
1  2017-03-24 15:00:14 CRIT(2) Land attack is blocked from (IP: 10.72.24.1 Port: 7)
GA-MLxxTPoE+#
```

2.6.10 clear attack-logging

This command is used to delete the attack log.

Syntax

- **clear attack-logging all**

Parameters

clear attack-logging all

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

This command used to delete the attack log messages.

Example

This example shows how to delete all the attack log messages.

```
GA-MLxxTPoE+# clear attack-logging all
GA-MLxxTPoE+#
```

2.7 System File Management Commands

2.7.1 boot config

This command is used to specify the file that will be used as the configuration file for the next boot.

Syntax

- **boot config** *FILE-PATH*

Parameters

Parameters	Description
FILE-PATH	Specifies the FILE-PATH of the file to be used as the startup configuration file.

Default

By default, the *config.cfg* file is used.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

The command is used to specify the startup configuration file. The default startup configuration file is *config.cfg*. If there is no valid configuration file, the device will be configured to the default state.

Example

This example shows how to configure the file 'switch-config.cfg' as the startup configuration file.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)# boot config switch-config.cfg
GA-MLxxTPoE+(config)#
```

2.7.2 boot image

This command is used to specify the file that will be used as the image file for the next boot.

Syntax

- **boot image [check]** *FILE-PATH*

Parameters

Parameters	Description
check	(Optional) Specifies to display the firmware information for the specified file. This information includes the version number and model description.
FILE-PATH	Specifies the FILE-PATH of the file to be used as the boot image file.

Default

By default, there is one image file as the boot image.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

When using the **boot image** command, the associated specified boot image file will be the startup boot image file for the next reboot. Use this command to assign a file as the next-boot image file. The system will check the model and checksum to determine whether the file is a valid image file.

The purpose of the **check** parameter is for checking the file information to let the user understand whether the specified file is suitable to be a boot image or not.
The setting of the **boot image** command will immediately be stored in the NVRAM, which is a space separated from the start-up configuration.
The backup image is decided automatically and is the newest valid image other than the boot-up one.

Example

This example shows how to specify that the Switch should use the image file named 'pnxxxxxx_v10000.rom' as the boot image file for the next startup.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# boot image pnxxxxxx_v10000.rom
GA-MLxxTPoE+(config)#
```

This example shows how to check a specified image file called "c:/ pnxxxxxx_v10000.rom". The checksum of the image file has been verified is okay and the information of the image file is displayed.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#boot image check pnxxxxxx_v10000.rom

----------------------
Image information
----------------------
Version: 1.0.0.00
Description: Panasonic Gigabit Ethernet Switch

GA-MLxxTPoE+(config)#
```

This example shows how to checks a specified image file called "pnxxxxxx_v10000_wrong.rom". The checksum of the image file has been verified wrong and an error message is displayed.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# boot image check pnxxxxxx_v10000_wrong.rom
ERROR: Invalid firmware image.
GA-MLxxTPoE+(config)#
```

2.7.3 clear running-config

This command is used to clear the system's running configuration.

Syntax

- **clear running-config**

Parameters

None

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to clear the system's configuration retained in DRAM. The configuration data will revert to the default settings. Before using this command, save a backup of the configuration using the **copy** command or upload the configuration profile to the TFTP server.
This command will clear the system's configuration settings, including IP parameters.Thus, all the existing remote connections will be disconnected. After this command was applied, the user needs to setup the IP address via the local console.

Example

This example shows how to clear the system's running configuration.

```
GA-MLxxTPoE+#clear running-config

This command will clear the system's configuration to the factory
default settings, including the IP address.
Clear running configuration? (y/n) [n] y

GA-MLxxTPoE+#
```

2.7.4 reset system

This command is used to reset the system, clear the system's configuration, then save and reboot the Switch.

Syntax

- **reset system**

Parameters

None

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to clear the system's configuration.The configuration data will revert to the default settings and then save it to the start-up configuration file and then reboot switch. Before using this command, save a backup of the configuration using the **copy** command or upload the configuration profile to the TFTP server.

Example

This example shows how to reset the system to the factory default settings.

```
GA-MLxxTPoE+#reset system

This command will clear the system's configuration to the factory
default settings, including the IP address.
Clear system configuration, save, reboot? (y/n) [n] y

Saving configurations and logs to NV-RAM......   Done


Please wait, the switch is rebooting...
```

2.7.5 copy

This command is used to copy a file to another file.

Syntax

- **copy** *SOURCE-URL DESTINATION-URL*
- **copy** *SOURCE-URL* {**tftp:** [*//LOCATION/DESTINATION-URL*] | **ftp:** [*//USER-NAME:PASSWORD@LOCATION:TCP-PORT/DESTINATION-URL*] | **rcp:** [*//USER-NAME@LOCATION/DESTINATION-URL*]}

- **copy** {**tftp:** [*//LOCATION/SOURCE-URL*] | **ftp:** [*//USER-NAME*:*PASSWORD*@*LOCATION*:*TCP-PORT/SOURCE-URL*] | **rcp:** [*//USER-NAME*@*LOCATION/SOURCE-URL*]} *DESTINATION-URL*

Parameters

Parameters	Description
SOURCE-URL	Specifies the source URL for the source file to be copied. One special form of the URL is represented by the following keywords. If **startup-config** is specified as the *SOURCE-URL*, the purpose is to upload the startup configuration, save the startup configuration as the file in the file system, or to execute the startup configuration as the running configuration. If **running-config** is specified as the *SOURCE-URL*, the purpose is to upload the running configuration or save the running configuration as the startup configuration or to save it as the file in the file system. If **local:** [*PATH-FILE-NAME*] is specified as the *SOURCE-URL*, the purpose is to specify the source file to be copied in the file system. If **log** is specified as the *SOURCE-URL*, the system log can be retrieved to the TFTP server or saved as the file in the file system. If **attack-log** *UNIT-ID* is specified as the *SOURCE-URL*, the purpose is to upload one unit's attack log.
DESTINATION-URL	Specifies the destination URL for the copied file. One special form of the URL is represented by the following keywords. If **running-config** is specified as the *DESTINATION-URL*, the purpose is to apply a configuration to the running configuration. If **startup-config** is specified as the *DESTINATION-URL*, the purpose is to save a configuration to the next-boot configuration. That is to keep the current configuration into the NVRAM and the file name will be the same as the file name specified with the **boot config** command. If **local:** [*PATH-FILE-NAME*] is specified as the *DESTINATION-URL*, the purpose is to specify the copied file in the file system. If the input absolute path is specified, the file will be downloaded to the place which of the absolute path indicates. If there is no unit information in the absolute path, the master unit will be assigned.
LOCATION	Specifies the IPv4 address the TFTP/FTP/RCP server, or IPv6 address of the TFTP/FTP server.
USER-NAME	Specifies the user name on the FTP/RCP server.
PASSWORD	Specifies the password for the user.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to copy a file to another file in the file system. Use this command to download or upload the configuration file or the image file. Use this command to upload the system log to the TFTP server. To upload the running configuration or save the running configuration to the startup configuration, specify **running-config** as the *SOURCE-URL*. To save the running configuration to the startup configuration, specify **startup-config** as the *DESTINATION-URL*.
As the destination is the startup configuration, the source file is directly copied to the file specified in the **boot config** command. Thus the original startup configuration file will be overwritten.
To apply a configuration file to the running configuration, specify **running-config** as the *DESTINATION-URL* for the **copy** command and the configuration file will be executed immediately by using the increment method. That means that the specified configuration will merge with the current running configuration. The running configuration will not be cleared before applying of the specified configuration.
As the specified source is the system log and the specified destination is a URL, the current system log will be copied to the specified URL.
To represent a file in the remote TFTP server, the URL must be prefixed with "tftp: //".
To download the firmware image, the user should use the **copy tftp: //** command to download the file from the TFTP server to a file in the file system. Then, use the **boot image** command to specify it as the boot image file.

Example

This example shows how to configure the Switch's running configuration by using the increment method using the configuration called "switch-config.cfg" that is download from the TFTP server 10.1.1.254.

```
GA-MLxxTPoE+#copy tftp: //10.1.1.254/switch-config.cfg running-config

Address of remote host [10.1.1.254]? 10.1.1.254
Source filename [switch-config.cfg]? switch-config.cfg
Destination filename running-config? [y/n]:  y

 Accessing tftp://10.1.1.254/switch-config.cfg...
 Transmission start...
 Transmission finished, file length 45421 bytes.

 Executing script file switch-config.cfg ......
 Executing done

GA-MLxxTPoE+#
```

This example shows how to upload the running configuration to the TFTP server for storage.

```
GA-MLxxTPoE+#copy running-config tftp: //10.1.1.254/switch-config.cfg

Address of remote host [10.1.1.254]? 10.1.1.254
Destination filename [switch-config.cfg]? switch-config.cfg
 Accessing tftp://10.1.1.254/switch-config.cfg...
 Transmission start...
 Transmission finished, file length 45421 bytes.

GA-MLxxTPoE+#
```

This example shows how to save the system's running configuration into the FLASH memory and uses it as the next boot configuration.

```
GA-MLxxTPoE+# copy running-config startup-config

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

GA-MLxxTPoE+#
```

This example shows how to execute the "switch-config.cfg" file in the NVRAM immediately by using the increment method.

```
GA-MLxxTPoE+# copy local: switch-config.cfg running-config

Source filename [switch-config.cfg]?
Destination filename running-config? [y/n]:  y

 Executing script file switch-config.cfg ......
 Executing done

GA-MLxxTPoE+#
```

This example shows how to download an image file from the TFTP server to unit.

```
GA-MLxxTPoE+#copy tftp: //10.1.1.254/pnxxxxxx_v10000.rom local: pnxxxxxx_v10000.rom

Address of remote host [10.1.1.254]?
Source filename [PN26xx9x_v0053.rom]?
Destination filename [pnxxxxxx_v10000.rom]?
 Accessing tftp://10.1.1.254/pnxxxxxx_v10000.rom...
 Transmission start...
 Transmission finished, file length 35562016 bytes.
 Please wait, programming flash.............. Done.

GA-MLxxTPoE+#
```

2.7.6 show boot

This command is used to display the boot configuration file and the boot image setting.

Syntax

- show boot

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command is used to display the boot configuration file and the boot image setting.

Example

This example shows how to display system boot information.

```
GA-MLxxTPoE+#show boot

 Boot image: /c:/pnxxxxxx_v10000.rom
 Boot config: /c:/config.cfg

GA-MLxxTPoE+#
```

2.7.7 show running-config

This command is used to display the commands in the running configuration file.

Syntax

- show running-config

Parameters

None

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 15

Usage Guideline

This command displays the current running system configuration.

Example

This example shows how to display the content of the running configuration file.

```
GA-MLxxTPoE+#show running-config
Building configuration...

Current configuration : 762 bytes

!-------------------------------------------------------------------------------

!                       GA-MLxxTPoE+ Gigabit Ethernet Switch
!                                  Configuration
!
!                              Firmware: Build V1.0.0.00
!                 Copyright(C) 2019 Panasonic. All rights reserved.
!-------------------------------------------------------------------------------

enable
config
!
spanning-tree mst configuration
 exit
!
line console
 exit
!
line ssh
 exit
--More--
```

2.7.8 show startup-config

This command is used to display the content of the startup configuration file.

Syntax

- show startup-config

Parameters

None

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 15

Usage Guideline

This command displays the configuration settings that the system will be initialized with.

Example

This example shows how to display the content of the startup configuration file.

```
GA-MLxxTPoE+#show startup-config

!-------------------------------------------------------------------------------

!                       GA-MLxxTPoE+ Gigabit Ethernet Switch
!                                 Configuration
!
!                             Firmware: Build V1.0.0.00
!                 Copyright(C) 2019 Panasonic. All rights reserved.
!-------------------------------------------------------------------------------
enable
config
!
spanning-tree mst configuration
 exit
!
line console
 exit
!
line ssh
 exit
!
line telnet
 exit
--More--
```

2.8 Time and Simple Network Time Protocol (SNTP) Commands

2.8.1 clock set

This command is used to manually set the system's clock.

Syntax

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

Parameters

Parameters	Description
HH:MM:SS	Specifies the current time in hours (24-hour format), minutes and seconds.
DAY	Specifies the current day (by date) in the month.
MONTH	Specifies the current month (by name, January, Jan, February, Feb, and so on).
YEAR	Specifies the current year (no abbreviation).

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

Generally, if the system is synchronized by a valid outside timing mechanism, such as SNTP, there is mp need to set the software clock. Use this command if no other time sources are available. The time specified in this command is assumed to be in the time zone specified by the configuration of the **clock timezone** command. The clock configured by this command will be applied to RTC if it is available. The configured clock will not be stored in the configuration file.
If the clock is manually set and the SNTP server is configured, the system will still try to sync the clock with the server. If the clock is manually set, but a new clock time is obtained by the SNTP server, the clock will be replaced by the new synced clock.

Example

This example shows how to manually set the software clock to 6:00 p.m. on Jul 4, 2017.

```
GA-MLxxTPoE+# clock set 18:00:00 4 jul 2017
GA-MLxxTPoE+#
```

2.8.2 clock summer-time

This command is used to configure the system to automatically switch to summer time (daylight saving time). Use the **no** form of this command to configure the Switch to not automatically switch over to summer time.

Syntax

- **clock summer-time recurring** *WEEK DAY MONTH HH:MM WEEK DAY MONTH HH:MM* [*OFFSET*]
- **clock summer-time date** *DATE MONTH YEAR HH:MM DATE MONTH YEAR HH:MM* [*OFFSET*]
- **no clock summer-time**

Parameters

Parameters	Description
recurring	Specifies that summer time should start and end on the specified week day of the specified month.
date	Specifies that summer time should start and end on the specified date of the specified month.
WEEK	Specifies the week of the month (1 to 4 or last).

Parameters	Description
DAY	Specifies the day of the week (sun, mon, and so on).
DATE	Specifies the date of the month (1 to 31).
MONTH	Specifies the current month. (by name, January, Jan, February, Feb, and so on)
YEAR	Specifies the start and end years for the summer time data.
HH:MM	Specifies the time (24 hours format) in hours and minutes.
OFFSET	(Optional) Specifies the number of minutes to add during summer time. The default value is 60. The range of this offset is 30, 60, 90 and 120.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to automatically switch over to summer time. The command has two forms. One is the recurring form which is used to specify the time through the week and the day of the month. The other form is the date form which is used to specify the date of the month.
In both the date and recurring forms of the command, the first part of the command specifies when summer time begins, and the second part specifies when it ends.

Example

This example shows how to specify that summer time starts on the first Sunday in April at 2 a.m. and ends on the last Sunday in October at 2 a.m.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# clock summer-time recurring 1 sun apr 2:00 last sun oct 2:00
GA-MLxxTPoE+(config)#
```

2.8.3 clock timezone

This command is used to set the time zone for display purposes. Use the **no** form of this command to set the time to the Coordinated Universal Time (UTC).

Syntax

- **clock timezone** {**+** | **-**} *HOURS-OFFSET* [*MINUTES-OFFSET*]
- **no clock timezone**

Parameters

Parameters	Description
+	Specifies that time to be added to UTC.
-	Specifies that time to be subtracted from UTC.
HOURS-OFFSET	Specifies the difference in hours from UTC.
MINUTES-OFFSET	(Optional) Specifies the difference in minutes from UTC.

Default

By default, this option is set to UTC +09:00.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The time obtained by the SNTP server refers to the UTC time. The local time will be calculated based on UTC time, time zone, and the daylight saving configuration.

Example

This example shows how to set the time zone to the Pacific Standard Time (PST), which is 8 hours ahead of UTC.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# clock timezone - 8
GA-MLxxTPoE+(config)#
```

2.8.4 show clock

This command is used to display the time and date information.

Syntax

- show clock

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command also indicates the clock's source. The clock source can be "No Time Source" or "SNTP".

Example

This example shows how to display the current time.

```
GA-MLxxTPoE+#show clock

     Current Time Source   :
     Current Time          : 05:56:45, 2000-01-30
     Time Zone             : UTC +00:00
     Daylight Saving Time  : Disabled

GA-MLxxTPoE+#
```

2.8.5 show sntp

This command is used to display information about the SNTP server.

Syntax

- show sntp

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command is used to display information about the SNTP server.

Example

This example shows how to display SNTP information.

```
GA-MLxxTPoE+#show sntp

SNTP Status               : Enabled
SNTP Poll Interval        : 720 sec

SNTP Server Status:

SNTP Server                                      Version Last Receive
------------------------------------------------ ------- ---------------
10.0.0.11                                        4       00:02:02
10::2                                            ------- ---------------
FE80::1111vlan1                                  ------- ---------------
------------------------------------------------ ------- ------- ---------------

Total Entries:3

GA-MLxxTPoE+#
```

2.8.6 sntp server

This command is used to allow the system clock to be synchronized with an SNTP time server. Use the **no** form of this command to remove a server from the list of SNTP servers.

Syntax

- **sntp server** {*IP-ADDRESS* | *IPV6-ADDRESS*}
- **no sntp server** {*IP-ADDRESS* | *IPV6-ADDRESS*}

Parameters

Parameters	Description
IP-ADDRESS	Specifies the IP address of the time server which provides the clock synchronization.
IPV6-ADDRESS	Specifies the IPv6 address of the time server.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

SNTP is a compact, client-only version of the NTP. Unlike NTP, SNTP can only receive the time from NTP servers; it cannot be used to provide time services to other systems. SNTP typically provides time within 100 milliseconds of the accurate time, but it does not provide the complex filtering and statistical mechanisms of NTP. In addition, SNTP does not authenticate traffic, although you can configure extended access lists to provide some protection.
Enter this command once for each NTP server. Configure the system with either this command or the **sntp broadcast client global configuration** command in order to enable SNTP. Create multiple SNTP servers by enter this command multiple times with different SNTP server IP addresses.

Use the **no** command to delete the SNTP server entry. To delete an entry, specify the information exactly the same as the originally configured setting. The time obtained from the SNTP server refers to the UTC time.

Example

This example shows how to configure a switch to allow its software clock to be synchronized with the clock by the SNTP server at IP address 192.168.22.44.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# sntp server 192.168.22.44
GA-MLxxTPoE+(config)#
```

2.8.7 sntp enable

This command is used to enable the SNTP function. Use the **no** form of this command to disable the SNTP function.

Syntax

- **sntp enable**
- **no sntp enable**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to enable or disable the SNTP function.

Example

This example shows how to enable the SNTP function.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# sntp enable
GA-MLxxTPoE+(config)#
```

2.8.8 sntp interval

This command is used to set the interval for the SNTP client to synchronize its clock with the server. Use the **no** form of this command to revert to the default setting.

Syntax

- **sntp interval** *SECONDS*
- **no sntp interval**

Parameters

Parameters	Description
SECONDS	Specifies the synchronization interval from 30 to 99999 seconds.

Default

By default, this value is 720 seconds.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to set the polling interval.

Example

This example shows how to configure the interval to 100 seconds.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# sntp interval 100
GA-MLxxTPoE+(config)#
```

2.9 Time Range Commands

2.9.1 periodic

This command is used to specify the period of time for a time range profile. This command is used in the time-range configuration mode. Use the **no** form of this command to remove the specified period of time.

Syntax

- **periodic** {**daily** *HH:MM* **to** *HH:MM* | **weekly** *WEEKLY-DAY HH:MM* **to** [*WEEKLY-DAY*] *HH:MM*}
- **no periodic** {**daily** *HH*:*MM* **to** *HH*:*MM* | **weekly** *WEEKLY-DAY HH*:*MM* **to** [*WEEKLY-DAY*] *HH*:*MM*}

Parameters

Parameters	Description
daily *HH:MM* **to** *HH:MM*	Specifies the time of the day, using the format HH:MM (for example, 18:30).
weekly *WEEK-DAY HH:MM* **to** [*WEEK-DAY*] *HH:MM*	Specifies the day of the week and the time of day in the format day HH:MM, where the day of the week is spelled out (monday, tuesday, wednesday, thursday, friday, saturday, and sunday). If the ending day of the week is the same as the starting day of the week, it can be omitted.

Default

None

Command Mode

Time-range Configuration Mode

Command Default Level

Level: 12

Usage Guideline

A new period can be partially overlapped with an older one. If a new period's starting and ending time is respectively the same as a previous period, an error message will be displayed and the new period will not be allowed. When specifying a period to remove, it must be the same period originally added and cannot be a partial range of a period or multiple periods configured. Otherwise, an error message will be displayed.

Example

This example shows how to create a time-range that include daily 09:00 to 12:00, 00:00 Saturday to 00:00 Monday and delete the period for daily 09:00 to 12:00.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# time-range rdtime
GA-MLxxTPoE+(config-time-range)# periodic daily 9:00 to 12:00
GA-MLxxTPoE+(config-time-range)# periodic weekly sat 00:00 to mon 00:00
GA-MLxxTPoE+(config-time-range)# no periodic daily 9:00 to 12:00
GA-MLxxTPoE+(config-time-range)#
```

2.9.2 show time-range

This command is used to display the time range profile configuration.

Syntax

- **show time-range** [*NAME*]

Parameters

Parameters	Description
NAME	(Optional) Specifies the name of the time-range profile to be displayed.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

If no optional parameter is specified, all configured time-range profiles will be displayed.

Example

This example shows how to display all the configured time ranges.

```
GA-MLxxTPoE+#show time-range

Time Range Profile: lunchtime
Daily 12:00 to 13:00

Time Range Profile: rdtime
Weekly Saturday   00:00 to Monday     00:00
Daily 09:00 to 12:00


Total Entries :2

GA-MLxxTPoE+#
```

2.9.3 time-range

This command is used to define a time-range profile and enter the time range configuration mode. Use the **no** form of this command to delete a time range.

Syntax

- **time-range** *NAME*
- **no time-range** *NAME*

Parameters

Parameters	Description
NAME	Specifies the name of the time-range profile to be configured. The maximum length is 32 characters.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to enter the time range configuration mode before using the **periodic** command to specify a time period. When a time-range is created without any time interval (periodic) setting, it implies that there is not any active period for the time-range and will not be displayed when issuing the **show time-range** command.

Example

This example shows how to enter the time range configuration mode for the time-range profile, named “rdtime”.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# time-range rdtime
GA-MLxxTPoE+(config-time-range)#
```

2.10 Fan Speed Setting

2.10.1 fanspeed

The **fanspeed** command is used to configure the rotational speed of fan. (The setting does not apply to the fan-less products.)

Syntax

- **fanspeed [high | low1 | low2 | min]**

Parameters

Parameter	Description
high	Specifies the rotational speed to high.
low1	Specifies the rotational speed to low.
low2	Specifies the rotational speed to low.
min	Specified the rotational speed to ultralow.

Default

The default is **high**.

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guideline

- This command is used to configure the rotational speed of fan and reduce the fan noise.
- By setting the rotational speed of fan, the maximum feeding power (Power Budget) will be automatically controlled.?Set the rotational speed of fan by considering the operation environment temperature and the maximum feeding power.

For the maximum feeding power to be controlled, refer to the operation manual or the product specification of each product.

- To display the rotational speed of fan, the **show peth-conf** command is used.

Example

This example shows how to configure the rotational speed of fan to ultralow.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#fanspeed min
GA-MLxxTPoE+(config)#
```

2.11 Reboot Commands

2.11.1 reboot

This command is used to reboot the Switch.

Syntax

- reboot [force_agree]

Parameters

Parameters	Description
force_agree	(Optional) Specifies to restart the Switch without confirmation.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 15

Usage Guideline

This command is used to reboot the Switch.

Example

This example shows how to reboot the Switch.

```
GA-MLxxTPoE+# reboot force_agree

Please wait, the switch is rebooting...
```

2.12 Cable Diagnostics Commands

2.12.1 test cable-diagnostics

This command is used to start the cable diagnostics to test the status and length of copper cables.

Syntax

- **test cable-diagnostics interface** *INTERFACE-ID* [, | -]

Parameters

Parameters	Description
interface *INTERFACE-ID*	Specifies the interface ID.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of interfaces. No space before and after the hyphen.

Default

None

Command Mode

EXEC Mode

Command Default Level

Level: 1

Usage Guideline

The command is available for physical port configuration. Cable Diagnostics can help users to detect whether the copper Ethernet port has connectivity problems. Use the **test cable-diagnostics** command to start the test. The copper port can be in one of the following status:

- **Open:** The cable in the error pair does not have a connection at the specified position.
- **Short:** The cable in the error pair has a short problem at the specified position.
- **Open or Short:** The cable has an open or short problem, but the PHY has no capability to distinguish between them.
- **Crosstalk:** The cable in the error pair has a crosstalk problem at the specified position.
- **Shutdown:** The remote partner is powered off.
- **Unknown:** The test got an unknown status.
- **OK:** The pair or cable has no error.
- **No cable:** The port does not have any cable connection to the remote partner.

Example

This example shows how to start the cable diagnostics to test the status and length of copper cables.

```
GA-MLxxTPoE+# test cable-diagnostics interface GigabitEthernet 1/0/1
GA-MLxxTPoE+#
```

2.12.2 show cable-diagnostics

This command is used to display the test results for the cable diagnostics.

Syntax

- **show cable-diagnostics [interface** *INTERFACE-ID* **[, | -]]**

Parameters

Parameters	Description
interface *INTERFACE-ID*	(Optional) Specifies the interface's ID. The acceptable interface will be a physical port.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of interfaces. No space before and after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command is used to display the test results for the cable diagnostics.

Example

This example shows how to display the test results for the cable diagnostics.

```
GA-MLxxTPoE+#show cable-diagnostics interface GigabitEthernet 1/0/1

Port      Type       Link Status   Test Result               Cable Length (M)
--------- ---------- ------------- ------------------------- -----------------
Gi1/0/1   1000BASE-T Link Down     OK                        2


GA-MLxxTPoE+#
```

2.12.3 clear cable-diagnostics

This command is used to clear the test results for the cable diagnostics.

Syntax

- **clear cable-diagnostics {all | interface** *INTERFACE-ID* **[, | -]}**

Parameters

Parameters	Description
all	Specifies to clear cable diagnostics results for all interfaces.
interface *INTERFACE-ID*	Specifies the interface's ID. The acceptable interface will be a physical port.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of interfaces. No space before and after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command is used to clear the test results for the cable diagnostics. If the test is running on the interface, an error message will be displayed.

Example

This example shows how to clear the test results for the cable diagnostics.

```
GA-MLxxTPoE+#clear cable-diagnostics interface GigabitEthernet 1/0/1
Clear cable-diagnostics for interfaces? (y/n) y
GA-MLxxTPoE+#
```

2.13 Digital Diagnostics Monitoring (DDM) Commands

2.13.1 show interfaces transceiver

This command is used to display the current SFP/SFP+ module operating parameters.

Syntax

- **show interfaces** [*INTERFACE-ID* [**,** | **-**] **transceiver** [**detail**]

Parameters

Parameters	Description
INTERFACE-ID	(Optional) Specifies multiple interfaces for transceiver monitoring status display. If no interface ID is specified, transceiver monitoring statuses on all valid interfaces are displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
detail	(Optional) Specifies to display more detailed information.

Default

None

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1

Usage Guideline

Use this command to display the current SFP/SFP+ module operating transceiver monitoring parameters values for specified ports.

Example

This example shows how to display current operating parameters for all ports valid for transceiver monitoring.

```
GA-MLxxTPoE+#show interfaces transceiver

 ++ : high alarm, +  : high warning, -  : low warning, -- : low alarm
 mA: milliamperes, mW: milliwatts

Transceiver Monitoring traps: None

           Temperature  Voltage      Bias Current TX Power     RX Power
port       (Celsius)    (V)          (mA)         (mW/dbm)     (mW/dbm)
---------- ------------ ------------ ------------ ------------ ------------
GigabitEthernet 1/0/21   33.247       3.294        8.049        0.572        0.000
                                                   -2.430         -
GigabitEthernet 1/0/22   35.551       3.269        7.974        0.601        0.001
                                                   -2.210       -29.089

Total Entries: 2

GA-MLxxTPoE+#
```

This example shows how to display detailed transceiver monitoring information for all ports which are valid for transceiver monitoring.

```
GA-MLxxTPoE+#show interfaces transceiver detail

 ++ : high alarm, +  : high warning, -  : low warning, -- : low alarm
 mA: milliamperes, mW: milliwatts
 A: The threshold is administratively configured.

GigabitEthernet 1/0/21
 Transceiver Monitoring is enabled
 Transceiver Monitoring shutdown action: None

                 Current      High-Alarm   High-Warning Low-Warning  Low-Alarm
Temperature(C)   33.172       78.000       73.000       -8.000       -13.000
Voltage(V)       3.293        3.700        3.600        3.000        2.900
Bias Current(mA) 8.059        11.800       10.800       5.000        4.000
TX Power(mW)     0.572        0.832        0.661        0.316        0.251
        (dbm)    -2.430       -0.800       -1.800       -5.000       -6.000
RX Power(mW)     0.000        1.000        0.794        0.016        0.010
        (dbm)       -         0.000        -1.000       -18.013      -20.000

GigabitEthernet 1/0/22
 Transceiver Monitoring is enabled
 Transceiver Monitoring shutdown action: None

                 Current      High-Alarm   High-Warning Low-Warning  Low-Alarm
Temperature(C)   35.422       78.000       73.000       -8.000       -13.000
--More--
```

2.13.2 snmp-server enable traps transceiver-monitoring

This command is used to enable the sending of all or individual optical transceiver monitoring SNMP notifications. Use the **no** form of this command to disable the sending of all or individual optical transceiver monitoring SNMP notifications.

Syntax

- **snmp-server enable traps transceiver-monitoring [alarm] [warning]**
- **no snmp-server enable traps transceiver-monitoring [alarm] [warning]**

Parameters

Parameters	Description
alarm	(Optional) Specifies to enable or disable the sending of alarm level notifications.
warning	(Optional) Specifies to enable or disable the sending of warning level notifications.

Default

By default, this feature is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

If no optional parameter is specified, it will enable or disable all transceiver-monitoring SNMP notifications.

Example

This example shows how to enable the sending of warning level notifications.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server enable traps transceiver-monitoring warning
GA-MLxxTPoE+(config)#
```

2.13.3 transceiver-monitoring action shutdown

This command is used to shut down a port from an alarm or a warning of an abnormal status. Use the **no** form of this command to disable the shutdown action.

Syntax

- **transceiver-monitoring action shutdown {alarm | warning}**
- **no transceiver-monitoring action shutdown**

Parameters

Parameters	Description
alarm	Specifies to shut down a port when alarm events occur.
warning	Specifies to shut down a port when warning events occur.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is available for physical port interface configuration.
The configuration can select to shut down a port on an alarm event or warning event or not to shut down on either of them. When the monitoring function is enabled, an alarm event occurs when the parameters, being monitored, go higher than the high alarm threshold or go lower than the low alarm threshold. A warning event occurs when the parameters being monitored go higher than the high warning threshold or go lower than the low warning threshold.
The port shutdown feature is controlled by the Error Disable module without a recover timer. Users can manually recover the port by using the **shutdown** command and then the **no shutdown** command.

Example

This example shows how to configure the shutdown GigabitEthernet 1/0/1 when an alarm event is detected.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface GigabitEthernet 1/0/1
GA-MLxxTPoE+(config-if)# transceiver-monitoring action shutdown alarm
GA-MLxxTPoE+(config-if)#
```

2.13.4 transceiver-monitoring bias-current

This command is used to configure the thresholds of the bias current for a specified port. Use the **no** form of this command to remove the configuration.

Syntax

- **transceiver-monitoring bias-current** *INTERFACE-ID* **{high | low} {alarm | warning}** *VALUE*
- **no transceiver-monitoring bias-current INTERFACE-ID {high | low} {alarm | warning}**

Parameters

Parameters	Description
INTERFACE-ID	Specifies the interface to modify.
high	Specifies the high threshold, when the operating parameter rises above this value. It indicates an abnormal status.
low	Specifies the low threshold, when the operating parameter falls below this value, It indicates an abnormal status.
alarm	Specifies the threshold for high alarm or low alarm conditions.
warning	Specifies the threshold for high warning or low warning conditions.
VALUE	Specifies the value of the threshold. This value is from 0 to 131 mA.

Default

None

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12

Usage Guideline

This configuration is only suitable for SFP+ port interfaces with optical modules with transceiver-monitoring.
This command configures the bias-current thresholds on the specified ports. The value will be stored both in the system and in the SFP/SFP+ transceivers and be converted to the 16-bit format and then rewritten into the SFP/SFP+ module.
If the SFP/SFP+ module being configured does not support the threshold change, the user-configured threshold is stored in the system and the displayed value will be the user-configured threshold. If no user-configured threshold exists, the displayed value will always reflect the factory preset value defined by vendors.
The **no** form of this command has the effect to clear the configured threshold stored in the system. It does not change the threshold stored in the SFP/SFP+ transceivers. Use the **no** form of the command to prevent threshold values on newly inserted SFP/SFP+ transceivers from being altered.

Example

This example shows how to configure the bias current high warning threshold as 10.237 on GigabitEthernet 1/0/21.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# transceiver-monitoring bias-current GigabitEthernet 1/0/21
high warning 10.237

WARNING: A closest value 10.236 is chosen according to the transceiver-monitoring
precision definition

GA-MLxxTPoE+(config)#
```

2.13.5 transceiver-monitoring enable

This command is used to enable the optical transceiver monitoring function for an SFP+ port. Use the **no** form of this command to remove disable optical transceiver monitoring.

Syntax

- **transceiver-monitoring enable**
- **no transceiver-monitoring enable**

Parameters

None

Default

By default, this option is enabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is available for the physical port interface configuration.
A user can use this command to enable or disable optical transceiver monitoring functions for an SFP+ port. When the monitoring function is enabled, an alarm event occurs when the parameters being monitored go higher than the high alarm threshold or go lower than the low alarm threshold. A warning event occurs when the parameters being monitored go higher than the high warning threshold or go lower than the low warning threshold.
When an SFP/SFP+ with transceiver monitoring capability is plugged into a port but the transceiver monitoring function of the port is disabled, the system will not detect the SFP/SFP+ transceiver's abnormal status but the user can still check the current status by showing the interface transceiver command.

Example

This example shows how to enable transceiver monitoring on GigabitEthernet 1/0/21.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface GigabitEthernet 1/0/21
GA-MLxxTPoE+(config-if)# transceiver-monitoring enable
GA-MLxxTPoE+(config-if)#
```

2.13.6 transceiver-monitoring rx-power

This command is used to configure the thresholds of the input power for the specified port. Use the **no** form of the command to remove the configuration.

Syntax

- transceiver-monitoring rx-power *INTERFACE-ID* {high | low} {alarm | warning} {mwatt *VALUE* | dbm *VALUE*}
- no transceiver-monitoring rx-power *INTERFACE-ID* {high | low} {alarm | warning}

Parameters

Parameters	Description
INTERFACE ID	Specifies the interface to modify.
high	Specifies that when the operating parameter rises above the highest threshold, it indicates an abnormal status
low	Specifies that when the operating parameter falls below the low threshold this value, it indicates an abnormal status.
alarm	Specifies to configure the high and low threshold value condition.
warning	Specifies to configure the high and low warning threshold conditions.
mwatt *VALUE*	Specifies the power threshold value in milliwatts. This value must be between 0 and 6.5535.
dbm *VALUE*	Specifies the power threshold value in dBm. This value must be between -40 and 8.1647.

Default

None

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12

Usage Guideline

Only SFP+ port interfaces with optical modules, with transceiver monitoring capability, are valid for this configuration.
This command configures the RX power thresholds on the specified port. This value will be stored both in the system and in the SFP/SFP+ transceivers and be converted to the 16-bit format and then written into the SFP/SFP+ module.

If the SFP/SFP+ module configured does not support the threshold change, the user-configured threshold is just stored in the system and the displayed value will be the user-configured threshold. If there is no user-configured threshold, the displayed value will always reflect the factory preset value defined by the vendor. The **no** form of this command has the effect to clear the configured threshold stored in system. It does not change the threshold stored in the SFP/SFP+ transceivers. Use **no** form of the command to prevent threshold values in newly inserted SFP/SFP+ transceivers from being altered.

Example

This example shows how to configure the RX power low warning threshold as 0.135 mW on GigabitEthernet 1/0/21.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# transceiver-monitoring rx-power GigabitEthernet 1/0/21 low warning mwatt 0.135
GA-MLxxTPoE+(config)#
```

2.13.7 transceiver-monitoring temperature

This command is used to configure the temperature thresholds for the specified port. Use the **no** form of this command to remove the configuration.

Syntax

- **transceiver-monitoring temperature** *INTERFACE-ID* **{high | low} {alarm | warning}** *VALUE*
- **no transceiver-monitoring temperature** *INTERFACE-ID* **{high | low} {alarm | warning}**

Parameters

Parameters	Description
INTERFACE ID	Specifies the interface to modify.
high	Specifies that when the operating parameter rises above this high threshold value, it indicates an abnormal status.
low	Specifies that when the operating parameter falls below this low threshold value, it indicates an abnormal status.
alarm	Specifies to configure the high and low threshold value condition.
warning	Specifies to configure the high and low warning threshold conditions.

Parameters	Description
VALUE	Specifies the threshold value. This value must be between -128 and 127.996 °C.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Only SFP+ port interfaces with optical modules, with transceiver monitoring capability, are valid for this configuration.
This command configures the RX power thresholds on the specified port. This value will be stored both in the system and in the SFP/SFP+ transceivers and be converted to the 16-bit format and then written into the SFP/SFP+ module.
If the SFP/SFP+ module configured does not support the threshold change, the user-configured threshold is just stored in the system and the displayed value will be the user-configured threshold. If there is no user-configured threshold, the displayed value will always reflect the factory preset value defined by the vendor.
The **no** form of this command has the effect to clear the configured threshold stored in system. It does not change the threshold stored in the SFP/SFP+ transceivers. Use the **no** form of the command to prevent threshold values in newly inserted SFP/SFP+ transceivers from being altered.

Example

This example shows how to configure the temperature high alarm threshold as 127.994 on GigabitEthernet 1/0/21.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# transceiver-monitoring temperature GigabitEthernet 1/0/21 high alarm 127.994

WARNING: A closer value of 127.992 is chosen according to the transceiver-monitoring precision definition

GA-MLxxTPoE+(config)#
```

2.13.8 transceiver-monitoring tx-power

This command is used to configure the output power threshold for the specified port. Use the **no** form of this command to remove the configuration.

Syntax

- **transceiver-monitoring tx-power** *INTERFACE-ID* {**high** | **low**} {**alarm** | **warning**} {**mwatt** *VALUE* | **dbm** *VALUE*}
- **no transceiver-monitoring tx-power** *INTERFACE-ID* {**high** | **low**} {**alarm** | **warning**}

Parameters

Parameters	Description
INTERFACE ID	Specifies the interface to modify.
high	Specifies the interface to modify.
low	Specifies that when the operating parameter rises above this high threshold value, it indicates an abnormal status.
alarm	Specifies that when the operating parameter falls below this low threshold value, it indicates an abnormal status.
warning	Specifies to configure the high and low warning threshold conditions.
mwatt *VALUE*	Specifies the power threshold value in milliwatts. This value must be between 0 and 6.5535.
dbm *VALUE*	Specifies the power threshold value in dBm. This value must be between -40 and 8.1647.

Default

None

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12

Usage Guideline

Only SFP+ port interfaces with optical modules, with transceiver monitoring capability, are valid for this configuration.
This command configures the TX power thresholds on the specified port. This value will be stored both in the system and in the SFP/SFP+ transceivers and be converted to the 16-bit format and then written into the SFP/SFP+ module.
If the SFP/SFP+ module configured does not support the threshold change, the user-configured threshold is just stored in the system and the displayed value will be the user-configured threshold. If there is no user-configured threshold, the displayed value will always reflect the factory preset value defined by the vendor.
The **no** form of this command has the effect to clear the configured threshold stored in system. It does not change the threshold stored in the SFP/SFP+ transceivers. Use the **no** form of the command to prevent threshold values in newly inserted SFP/SFP+ transceivers from being altered.

Example

This example shows how to configure the TX power low warning threshold to 0.181 mW on GigabitEthernet 1/0/21.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# transceiver-monitoring tx-power GigabitEthernet 1/0/21 low warning mwatt 0.181
GA-MLxxTPoE+(config)#
```

2.13.9 transceiver-monitoring voltage

This command is used to configure the threshold voltage of the specified port. Use the **no** form of this command to remove the configuration.

Syntax

- **transceiver-monitoring voltage** *INTERFACE-ID* **{high | low} {alarm | warning}** *VALUE*
- **no transceiver-monitoring voltage** *INTERFACE-ID* **{high | low} {alarm | warning}**

Parameters

Parameters	Description
INTERFACE-ID	Specifies the interface to modify.
high	Specifies that when the operating parameter rises above the highest threshold, it indicates an abnormal status.

Parameters	Description
low	Specifies that when the operating parameter falls below this low threshold value, it indicates an abnormal status.
alarm	Specifies to configure the high and low threshold value condition.
warning	Specifies to configure the high and low warning threshold conditions.
VALUE	Specifies the threshold value. This value must be between 0 and 6.5535 Volt.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Only SFP+ port interfaces with optical modules, with transceiver monitoring capability, are valid for this configuration.
This command configures the voltage thresholds on the specified port. The value will be stored both in the system and in the SFP/SFP+ transceivers and be converted to the 16-bit format and then written into the SFP/SFP+ module.
If the SFP/SFP+ module configured does not support the threshold change, the user-configured threshold is just stored in the system and the displayed value will be the user-configured threshold. If there is no user-configured threshold, the displayed value will always reflect the factory preset value defined by the vendor.
The **no** form of this command has the effect to clear the configured threshold stored in system. It does not change the threshold stored in the SFP/SFP+ transceivers. Use the **no** form of the command to prevent threshold values in newly inserted SFP/SFP+ transceivers from being altered.

Example

This example shows how to configure the low alarm voltage threshold as 0.005 on GigabitEthernet 1/0/21.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# transceiver-monitoring voltage GigabitEthernet 1/0/21 low alarm
0.005
GA-MLxxTPoE+(config)#
```

2.14 OAM (Operations, Administration, Maintenance)

2.14.1 ethernet oam

This command is used to enable the Ethernet OAM on the specified interface. Use the **no** command of this command to disable it.

Syntax

- **ethernet oam [max-rate** *OAM-PDUS* **| min-rate** *SECONDS* **| mode { active | passive } | timeout** *SECONDS* **]**
- **no ethernet oam [max-rate | min-rate | mode | timeout]**

Parameters

Parameter	Description
max-rate *OAM-PDUS*	Specifies the maximum number of OAM PDUs transmitted every second. The range is from 1 to 10. The default is 10.
min-rate *SECONDS*	Specifies the minimum transmission rate in seconds. The range is from 1 and 10 seconds. The default is 1 second.
mode	Specifies the OAM client mode.
active	Specifies the OAM client mode to active. The default is active mode.
passive	Specifies the OAM client mode to passive.
timeout *SECONDS*	Specifies the timeout value of the OAM client. The range is from 2 and 30 seconds. The default is 5 seconds.

Default

max-rate: 10
min-rate: 1 sec
mode : **active**
timeout : 5 sec

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The OAM function is used to monitor the line state between neighboring devices. This command is used to change the Ethernet OAM parameter on the specified interface.

Example

This example shows how to enable the Ethernet OAM on the interface G1/0/1.

```
GA-MLxxTPoE+>enable
GA-MLxxTPoE+#configure
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#ethernet oam
```

2.14.2 ethernet oam remote-loopback

This command is used to enable the Ethernet OAM remote-loopback or to configure the loopback timeout on the interface. Use the **no** form of this command to disable the Ethernet OAM function or to delete the timeout settings.

Syntax

- **ethernet oam remote-loopback {supported | timeout** *SECONDS*}
- **no ethernet oam remote-loopback {supported | timeout }**

Parameters

Parameter	Description
supported	Enables the remote-loopback.
timeout *SECONDS*	Specifies the timeout of remote-loopback. The range is from 1 and 10 seconds. The default is 10 seconds.

Default

supported: By default, this feature is disabled.
timeout: The default is 10 seconds.

Command Mode

Interface Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to enable the Ethernet OAM remote-loopback or to configure the loopback timeout on the interface.

Example

This example shows how to enable the remote-loopback function of Ethernet OAM on the interface Gi1/0/1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#ethernet oam remote-loopback supported
GA-MLxxTPoE+(config-if)#no ethernet oam remote-loopback supported
GA-MLxxTPoE+(config-if)#
```

2.14.3 ethernet oam remote-loopback interface

This command is used to start or to end the remote-loopback on the specified interface.

Syntax

- **ethernet oam remote-loopback interface** *INTERFACE* **{ start | stop}**

Parameters

Parameter	Description
INTERFACE	Specifies the interface to perform the remote-loopback.
start	Starts the remote-loopback.
stop	Ends the remote-loopback.

Default

N/A

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to start or end the remote-loopback on the specified interface.

Example

This example shows how to start the remote-loopback on the interface Gi1/0/1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+#ethernet oam remote-loopback interface gi 1/0/1 start
While you test Ethernet OAM MAC connectivity,
you will be unable to pass traffic across this link.
Are you sure to turn on remote loopback? [Y/N]
y

GA-MLxxTPoE+#
```

This example shows how to end the remote-loopback on the interface Gi1/0/1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+#ethernet oam remote-loopback interface gi 1/0/1 stop
January 23 03:23:26 Interface Gi1/0/1 has exited the Ethernet OAM loopback mode.

GA-MLxxTPoE+#
```

2.14.4 ethernet oam link-monitor supported

This command is used to enable the link monitor of Ethernet OAM on the specified interface. Use the **no** form of the command to remove the configuration.

Syntax

- **ethernet oam link-monitor supported**
- **no ethernet oam link-monitor supported**

Parameters

N/A

Default

The default is enabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to enable the link monitor of Ethernet OAM on the specified interface. Use the **no** form of the command to remove the configuration.

Example

This example shows how to enable the link monitor of Ethernet OAM on the interface Gi1/0/1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)# ethernet oam link-monitor supported
```

2.14.5 ethernet oam link-monitor frame

This command is used to enable the error frame check of the Ethernet OAM link monitor on the specified interface. Use the **no** form of this command to disable it.

Syntax

- **ethernet oam link-monitor frame** {**threshold** {**high** *HIGH-FRAMES* | **none** } | **low** *LOW-FRAMES* } | **window** *MILLISECONDS* }
- **no ethernet oam link-monitor frame** {**threshold** {**high** | **low** } | **window** }

Parameters

Parameter	Description
threshold	Specifies the threshold value of the error frame.
high *HIGH-FRAMES*	Specifies the high threshold of the error frame. The range is from 1 to 65535 The default is none.
none	Disables the high threshold.
low *LOW-FRAMES*	Specifies the low threshold of the error frame. The range is from 0 to 65535 The default is 10.
window *MILLISECONDS*	Specifies the window size of the error frame count period. The range is from 10 to 600 milliseconds. The value is hundredfold of milliseconds value. The default is 100 milliseconds.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to enable the error frame check of the Ethernet OAM link monitor on the specified interface.

Example

This example shows how to specify the threshold of upper error frame to 100 and the threshold of lower error frame to 80 on the interface Gi 1/0/1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface GigabitEthernet 1/0/1
GA-MLxxTPoE+(config-if)#ethernet oam link-monitor frame threshold high 100
GA-MLxxTPoE+(config-if)#ethernet oam link-monitor frame threshold low 80
```

2.14.6 ethernet oam link-monitor frame-period

This command is used to enable the monitoring which is triggered by the number of error frames which occurred during the error frame period of the Ethernet OAM link monitor on the specified interface. Use the **no** form of this command to disable it.

Syntax

- **ethernet oam link-monitor frame-period {threshold {high** *HIGH-FRAMES* **| none } | low** *LOW-FRAMES* **} | window** *MILLISECONDS* **}**
- **no ethernet oam link-monitor frame {threshold {high | low } | window }**

Parameters

Parameter	Description
threshold	Specifies the threshold value of the error frame time.
high *HIGH-FRAMES*	Specifies the high threshold of the error frame time. The range is from 1 to 65535. The default is none.
none	Disables the high threshold.
low *LOW-FRAMES*	Specifies the low threshold of the error frame time. The range is from 0 to 65535 The default is 1.
window *MILLISECONDS*	Specifies the window size of the polling time. The range is from 10 to 1800 milliseconds. The value is hundredfold of milliseconds value. The default is 100 milliseconds.

Default

N/A

Command Mode

Interface Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to enable the monitoring which is triggered by the number of error frames which occurred during the error frame period of the Ethernet OAM link monitor on the specified interface.

Example

This example shows how to specify the threshold of upper error frame to 100 and the threshold of lower error frame to 80 on the interface Gi 1/0/1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface GigabitEthernet 1/0/1
GA-MLxxTPoE+(config-if)#ethernet oam link-monitor frame-period threshold high 100
GA-MLxxTPoE+(config-if)#ethernet oam link-monitor frame-period threshold low 80
```

2.14.7 ethernet oam link-monitor recv-crc

This command is used to set the threshold value which is used to monitor the input frame with a CRC error on the specified interface. Use the **no** form of this command to disable it.

Syntax

- **ethernet oam link-monitor recv-crc** {**threshold** {**high** *HIGH-FRAMES* | **none** } | **low** *LOW-FRAMES* } | **window** *FRAMES* }
- **no ethernet oam link-monitor recv-crc** {**threshold** {**high** | **low** } | **window** }

Parameters

Parameter	Description
threshold	Specifies the threshold value of the error frame with a CRC error.
high *HIGH-FRAMES*	Specifies the high threshold of the error frame. The range is from 1 to 65535. The default is none.
none	Disables the high threshold.
low *LOW-FRAMES*	Specifies the low threshold of the error frame. The range is from 0 to 65535. The default is 1.
window *FRAMES*	Specifies the window size of the polling time. The range is from 10 to 1800. The default is 100.

Default

N/A

Command Mode

Interface Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to set the threshold value which is used to monitor the input frame with a CRC error on the specified interface.

Example

This example shows how to specify the high threshold of CRC error frame to 100 and the low threshold of error frame to 80 on the interface Gi 1/0/1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface GigabitEthernet 1/0/1
GA-MLxxTPoE+(config-if)#ethernet oam link-monitor recv-crc threshold high 100
GA-MLxxTPoE+(config-if)#ethernet oam link-monitor recv-crc threshold low 80
```

2.14.8 ethernet oam action

This command is used to configure whether to perform the error disable when an error event occurs. When the error disable is performed, the interface performs shutdown. Use the **no** form of this command to set it back.

Syntax

- **ethernet oam actoin {high-threshold | dying-gasp} error-disbale-interface**
- **no ethernet oam actoin {high-threshold | dying-gasp} error-disbale-interface**

Parameters

Parameter	Description
high-threshold	Specifies to shut down the interface when the high threshold is exceeded.
dying-gasp	Specifies to shut down the interface when Dying-Gasp is received.

Default

N/A

Command Mode

Interface Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to configure whether or not to perform the error disable when an error event occurs.

Example

This example shows how to disable the interface by the error disable when the high threshold is exceeded on the interface Gi 1/0/1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface GigabitEthernet 1/0/1
GA-MLxxTPoE+(config-if)#ethernet oam action high-threshold error-disbale-interface
```

2.14.9 show ethernet oam configuration

This command is used to display the configuration of Ethernet OAM.

Syntax

- **show ethernet oam configuration** [**interface** INTERFACE]

Parameters

Parameter	Description
INTERFACE	Specifies to display the configuration of Ethernet OAM to the specified interface.

Default

N/A

Command Mode

Privileged Mode

Command Default Level

Level:1

Usage Guideline

This command is used to display the configuration of Ethernet OAM.

Example

This example shows how to display the configuration of Ethernet OAM.

```
GA-MLxxTPoE+#show ethernet oam configuration

Interface Ethernet OAM Remote Loopback Link monitoring
--------- ------------ --------------- ---------------
Gi1/0/1   Enabled      Supported       Supported
Gi1/0/2   Disabled     Not Supported   Supported
Gi1/0/3   Disabled     Not Supported   Supported
Gi1/0/4   Disabled     Not Supported   Supported
Gi1/0/5   Disabled     Not Supported   Supported
Gi1/0/6   Disabled     Not Supported   Supported
```

This example shows how to display the configuration of Ethernet OAM on the interface Gi1/0/1.

```
GA-MLxxTPoE+#show ethernet oam configuration interface gi 1/0/1

General
   Interface              : Gi1/0/1
   Admin Status           : Enabled
   Mode                   : Active
   PDU Max Rate           : 10 packets per second
   PDU Min Rate           : 1 packet per 10 second
   Link Timeout           : 5
   High-Threshold Action  : Error-disable-interface
   Dying-gasp Action      : None

Remote Loopback
   Status                 : Supported
   Timeout                : 10

Link monitoring
   Status                 : Supported
   frame Error
      Window              : 100 x 100 milliseconds
      Low Threshold       : 80 error frames
      High Threshold      : 1000 error frames

   frame Period Error
      Window              : 1000 x 10000 frames
      Low Threshold       : 80 error frames
      High Threshold      : 100 error frames

   Receive-Frame CRC Error
      Window              : 1000 x 100 milliseconds
      Low Threshold       : 10 error frames
      High Threshold      : None
```

2.14.10 show ethernet oam discovery

This command is used to display the discovery information of Ethernet OAM.

Syntax

- **show ethernet oam discovery [interface** INTERFACE **]**

Parameters

Parameter	Description
INTERFACE	Specifies to display the configuration of Ethernet OAM to the specified interface.

Default

N/A

Command Mode

Privileged Mode

Command Default Level

Level:1

Usage Guideline

This command is used to display the discovery information of Ethernet OAM.

Example

This example shows how to display the configuration of Ethernet OAM.

```
GA-MLxxTPoE+#show ethernet oam discovery

Interface Ethernet OAM Remote MAC Address
--------- ------------ ------------------
Gi1/0/1   Enabled      00-C0-8F-01-01-01
Gi1/0/2   Disabled
Gi1/0/3   Disabled
Gi1/0/4   Disabled
Gi1/0/5   Disabled
Gi1/0/6   Disabled
```

This example shows how to display the discovery information of Ethernet OAM on the interface Gi1/0/1.

```
GA-MLxxTPoE+#show ethernet oam discovery interface gi 1/0/1

Local Client
   Interface              : Gi1/0/1
   Admin Status           : Enabled
   Mode                   : Active
   Remote Loopback        : Supported
   Link Monitoring        : Supported
   PDU Revision           : 3

Remote Client
   MAC Address            : 00-00-00-00-00-00
   PDU revision           : 0
   Mode                   : Unknown
   Remote Loopback        : Not Supported
   Remote Loopback state  : None
   Link Monitoring        : Not Supported
```

2.14.11 show ethernet oam statistics

This command is used to display the statistics information of PDU transmission/ reception of Ethernet OAM.

Syntax

- **show ethernet oam discovery [interface** INTERFACE **]**

Parameters

Parameter	Description
INTERFACE	Specifies to display the statistics information of Ethernet OAM to the specified interface.

Default

N/A

Command Mode

Privileged Mode

Command Default Level

Level:1

Usage Guideline

This command is used to display the statistics information of PDU transmission/reception of Ethernet OAM.

Example

This example shows how to display the statistics information of PDU transmission/reception of Ethernet OAM.

```
GA-MLxxTPoE+#show ethernet oam statistics

Interface OAMPDU TX OAMPDU RX Local Fault Remote Fault Local Event Remote Event
--------- --------- --------- ----------- ------------ ----------- ------------
Gi1/0/1   0         0         0           0            0           0
Gi1/0/2   0         0         0           0            0           0
Gi1/0/3   0         0         0           0            0           0
Gi1/0/4   0         0         0           0            0           0
Gi1/0/5   0         0         0           0            0           0
Gi1/0/6   0         0         0           0            0           0
```

This example shows how to display the statistics information of PDU transmission/reception of Ethernet OAM on the interface Gi1/0/1.

```
GA-MLxxTPoE+#show ethernet oam statistics interface gi 1/0/1

Interface : Gi1/0/1
Counter
   Information OAMPDU TX        : 0
   Information OAMPDU RX        : 0
   Event Notification OAMPDU TX : 0
   Event Notification OAMPDU RX : 0
   Loopback Control OAMPDU TX   : 0
   Loopback Control OAMPDU RX   : 0
   Unsupported OAMPDU TX        : 0
   Unsupported OAMPDU RX        : 0

Local Fault
   Link Fault Records           : 0
   Dying Gasp Records           : 0

Remote Fault
   Link Fault Records           : 0
   Dying Gasp Records           : 0

Local Events
   Errored Frame Records        : 0
   Errored Frame Period Records : 0
   Errored CRC Records          : 0

Remote Events
   Errored Frame Records        : 0
   Errored Frame Period Records : 0
   Errored CRC Records          : 0
```

2.15 CFM (Connectivity Fault Management)

2.15.1 cfm enable

This command is used to enable the global configuration of CFM function.

Syntax

- cfm enable
- no cfm enable

Parameters

N/A

Default

By default, the global configuration is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The CFM function is used to monitor the connection state between multiple devices.
This command is used to enable the global configuration of CFM function.

Example

This example shows how to enable the global configuration of CFM function.

```
GA-MLxxTPoE+>enable
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#cfm enable
```

2.15.2 cfm domain

This command is used to create a maintenance domain (MD). If a created or specified domain exists, use the **no** form of this command to delete the maintenance domain (MD).

Syntax

- **cfm domain** *DOMAIN-NAME*
- **no cfm domain**

Parameters

Parameter	Description
DOMAIN-NAME	Specifies the domain name, with a maximum of 43 characters.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to create a maintenance domain (MD).

Example

This example shows how to create a maintenance domain (MD).

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#cfm domain test1
GA-MLxxTPoE+(config-cfm)#
```

2.15.3 level

This command is used to configure the level of maintenance domain (MD). Use the **no** form of the command to remove the configuration.

Syntax

- **level** *LEVEL-ID*

Parameters

Parameter	Description
LEVEL-ID	Specifies the domain level. The range is from 0 to 7.

Default

N/A

Command Mode

CFM Configuration Mode

Command Default Level

Level:12

Usage Guideline

This configuration is only suitable for SFP+ port interfaces with optical modules with transceiver-monitoring.

Example

This example shows how to create a domain "Customer" and set the level to 7.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#cfm domain Customer
GA-MLxxTPoE+(config-cfm)#level 7
```

2.15.4 service

This command is used to create a maintenance association (MA). Use the **no** form of this command.

Syntax

- **servive** *MA-NAME*
- **no service**

Parameters

Parameter	Description
MA-NAME	Specifies the MA name, with a maximum of 12 characters.

Default

By default, this option is disabled.

Command Mode

CFM Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to create a maintenance association (MA).

Example

This example shows how to create a maintenance association (MA).

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#cfm domain Customer
GA-MLxxTPoE+(config-cfm)#service CustomerMA
```

2.15.5 continuity-check

This command is used to configure the continuity check messages (CCM). Use the **no** form of the command to remove the configuration.

Syntax

- **continuity-check** [*INTERVAL*]
- **no continuity-check**

Parameters

Parameter	Description
INTERVAL	Specifies the transmission interval of CC messages.

Default

N/A

Command Mode

CFM MA Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to configure the continuity check messages (CCM).

Example

This example shows how to configure the interval of continuity check messages (CCM) to 100 ms.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+#(config)#cfm domain Customer
GA-MLxxTPoE+(config-cfm)#service CustomerMA
GA-MLxxTPoE+(config-cfm-srv)#continuity-check 100ms
```

2.15.6 cfm mep mepid

This command is used to configure the maintenance intermediate point (MIP) for the domain level ID. Use the **no** form of the command to remove the configuration.

Syntax

- **transcfm mep mepid** *MEP-ID* **level** *LEVEL-ID* **service** *SERVICE-NAME* **vlan** {*VLAN-ID* {[inword] | outward} {remote}}

Parameters

Parameter	Description
MEP-ID	Specifies the MIP ID.
LEVEL-ID	Specifies the MIP level.
SERVICE-NAME	Specifies the service name.
VLAN-ID	Specifies the VLAN name.
inword	Specifies the input direction of MEP.
outward	Specifies the output direction of MEP.
remote	Specifies the remote MEP.

Default

N/A

Command Mode

Interface Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to configure the maintenance intermediate point (MIP) for the domain level ID.

Example

This example shows how to configure the maintenance intermediate point (MIP) for the domain level ID on the interface Gi1/0/1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#int gi1/0/1
GA-MLxxTPoE+(config-if)#cfm mep mep-id 1 level 7 service customerMA vlan 1 inwar
d
```

2.15.7 show cfm

This command is used to display the information of maintenance domain (MD).

Syntax

- show cfm

Parameters

N/A

Default

N/A

Command Mode

Privileged Mode

Command Default Level

Level:1

Usage Guideline

This command is used to display the information of maintenance domain (MD).

Example

This example shows how to display the information of maintenance domain (MD).

```
GA-MLxxTPoE+#show cfm

 Global Status : Enabled
 Total Entries : 0

Domain Name                                Level No. of MA
------------------------------------------ ----- ---------
```

2.15.8 show cfm domain

This command is used to display the list of maintenance associations (MAs).

Syntax

- **show cfm domain** *DOMAIN-NAME*

Parameters

Parameter	Description
DOMAIN-NAME	Displays the CFM domain.

Default

N/A

Command Mode

Privileged Mode

Command Default Level

Level:1

Usage Guideline

This command is used to display the list of maintenance associations (MAs).

Example

This example shows how to display the list of maintenance associations (MAs).

```
GA-MLxxTPoE+#show cfm domain cunstomer

 Domain         : customer
 Level          : 1

 Total Entries : 0

MA Name
-----------------------------------------
```

2.15.9 show cfm service

This command is used to display the information of maintenance association (MA).

Syntax

- **show cfm service** [*MA-NAME*]

Parameters

Parameter	Description
MA-NAME	Specifies to display the detailed information of the specified MA entry.

Default

N/A

Command Mode

Privileged Mode

Command Default Level

Level:1

Usage Guideline

This command is used to display the information of maintenance association (MA).

Example

This example shows how to display the information of maintenance association (MA).

```
GA-MLxxTPoE+#show cfm service

 Total Entries: 0

Name                                     Level
---------------------------------------- -----
```

2.15.10 show cfm mip

This command is used to display the information of maintenance intermediate point (MIP).

Syntax

- show cfm mip

Parameters

N/A

Default

N/A

Command Mode

Privileged Mode

Command Default Level

Level:1

Usage Guideline

This command is used to display the information of maintenance intermediate point (MIP).

Example

This example shows how to display the information of maintenance intermediate point (MIP).

```
GA-MLxxTPoE+#show cfm mip

 Total Entries: 0

Index Interface LEVEL VLAN
----- --------- ----- ----
```

2.15.11 show cfm mep local

This command is used to display the detailed information of local MEP entry.

Syntax

- **show cfm mep local [mepid** *MEP-ID* **]**

Parameters

Parameter	Description
mepid *MEP-ID*	Specifies to display the detailed information of local MEP entry.

Default

N/A

Command Mode

Privileged Mode

Command Default Level

Level:1

Usage Guideline

This command is used to display the detailed information of local MEP entry.

Example

This example shows how to display the detailed information of local MEP entry.

```
GA-MLxxTPoE+#show cfm mep local

 Total Entries: 0

MEPID Interface Domain Name                                CC status
----- --------- ---------------------------------------- ---------
```

2.15.12 show cfm mep remote

This command is used to display the information of remote MEP.

Syntax

- **show cfm mep remote [mepid** *MEP-ID* **]**

Parameters

Parameter	Description
mepid *MEP-ID*	Specifies to display the detailed information of remote MEP entry.

Default

N/A

Command Mode

Privileged Mode

Command Default Level

Level:1

Usage Guideline

This command is used to display the information of remote MEP.

Example

This example shows how to display the information of remote MEP.

```
GA-MLxxTPoE+#show cfm mep remote

 Total Entries: 0

MEPID Interface LEVEL CC status
----- --------- ----- ---------
```

2.16 Debug Commands

2.16.1 debug show tech-support

This command is used to display the information required by technical support personnel.

Syntax

- debug show tech-support

Parameters

None

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to display technical support information. The technical support information is used to collect the Switch's information needed by the engineers to troubleshoot or analyze a problem.

Example

This example shows how to display technical support information of all the modules.

```
ZGA-MLxxTPoE+#debug show tech-support

#-------------------------------------------------------------------------------
#                       GA-MLxxTPoE+ Gigabit Ethernet Switch
#                          Technical Support Information
#
#                             Firmware: Build V1.0.0.00
#        Copyright(C) 2019  Panasonic. All rights reserved.
#-------------------------------------------------------------------------------


********************   show clock   ********************

     Current Time Source   :
     Current Time          : 13:39:50, 2019-05-21
     Time Zone             : UTC +09:00
     Daylight Saving Time  : Disabled


********************   show unit   ********************

Unit: 1
Model Descr: xP 10/100/1000 with xP Combo
Product Name: GA-MLxxTPoE+
--More--
```

3 Interface

3.1 Interface Commands

3.1.1 clear counters

This command is used to clear counters for the specified interfaces.

Syntax

- **clear counters** {**all** | **interface** *INTERFACE-ID* [**,** | **-**]}

Parameters

Parameters	Description
all	Specifies to clear counters for all interfaces.
interface *INTERFACE-ID*	Specifies the interfaces to be configured. The interfaces can be physical ports, the OOB management port, port-channels or Layer 2 VLAN interfaces.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to clear counters for a physical port interface.

Example

This example shows how to clear the counters of GigabitEthernet 1/0/1.

```
GA-MLxxTPoE+# clear counters interface GigabitEthernet 1/0/1
GA-MLxxTPoE+#
```

3.1.2 description

This command is used to add a description to an interface. Use the **no** form of this command to delete the description.

Syntax

- **description** *STRING*
- **no description**

Parameters

Parameters	Description
STRING	Specifies a description for an interface with a maximum of 64 characters.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The specified description corresponds to the MIB object “ifAlias” defined in the RFC 2233.

Example

This example shows how to add the description “Physical Port 10” to interface GigabitEthernet 1/0/10.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface GigabitEthernet 1/0/10
GA-MLxxTPoE+(config-if)# description Physical Port 10
GA-MLxxTPoE+(config-if)#
```

3.1.3 interface

This command is used to enter the interface configuration mode for a single interface. Use the **no** form of this command to remove an interface.

Syntax

- **interface** *INTERFACE-ID*
- **no interface** *INTERFACE-ID*

Parameters

Parameters	Description
INTERFACE-ID	Specifies the ID of the interface. The interface ID is formed by interface type and interface number with no spaces in between.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to enter the interface configuration mode for a specific interface. The interface ID is formed by the interface type and interface number with no spaces in between.

The following keywords can be used for the supported interface types:

- **Ethernet** - Specifies the physical Ethernet switch port with all different media.
- **Port-channel** - Specifies the aggregated port-channel interface.
- **VLAN** - Specifies the VLAN interface.

The format of the interface number is dependent on the interface type.
For physical port interfaces, the user cannot enter the interface if the Switch port does not exist. The physical port interface cannot be removed by the **no** command.
Use the **interface VLAN** command to create Layer 3 interfaces. Use the **VLAN** command in the global configuration mode to create a VLAN before creating Layer 3 interfaces. Use the **no interface VLAN** command to remove a Layer 3 interface.
The port-channel interface is automatically created when the **channel-group** command is configured for the physical port interface. The port-channel interface is automatically removed when no physical port interface has the **channel-group** command configured on it.

Example

This example shows how to enter the interface configuration mode for the GigabitEthernet 1/0/5.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface GigabitEthernet 1/0/5
GA-MLxxTPoE+(config-if)#
```

This example shows how to enter the interface configuration mode for VLAN 100.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface vlan100
GA-MLxxTPoE+(config-if)#
```

This example shows how to enter the interface configuration mode for port-channel 3.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface port-channel3
GA-MLxxTPoE+(config-if)#
```

3.1.4 interface range

This command is used to enter the interface range configuration mode for multiple interfaces.

Syntax

- interface range *INTERFACE-ID* [, | -]

Parameters

Parameters	Description
INTERFACE-ID	Specifies the ID of the interface. The interface ID is formed by interface type and interface number with no spaces in between.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command enters the interface configuration mode for the specified range of interfaces. Commands configured in the interface range mode, applies to interfaces in the range.

Example

This example shows how to enter the interface configuration mode for the range of ports 1/0/1 to 1/0/5: and port 1/0/7.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface range GigabitEthernet 1/0/1-5,1/0/7
GA-MLxxTPoE+(config-if-range)#
```

3.1.5 show counters

This command is used to display interface information.

Syntax

- **show counters** [**interface** *INTERFACE-ID*]

Parameters

Parameters	Description
interface *INTERFACE-ID*	(Optional) Specifies that the interface can be a physical port, port channel or VLAN interfaces. If no interface is specified, counters of all interfaces will be displayed.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display the statistic counters for an interface.
The following items provide you with details on the display parameters of this command:

- **max-rcv-frame-size:** indicates the maximum Ethernet frame size, which is defined in **Jumbo Frame Commands**. The range is from 64 to 9216 bytes.

Example

This example shows how to display the counters for GigabitEthernet1/0/1.

```
GA-MLxxTPoE+#show counters interface GigabitEthernet 1/0/1

GigabitEthernet 1/0/1 counters
rxHCTotalPkts                       : 67004
txHCTotalPkts                       : 63918
rxHCUnicastPkts                     : 66026
txHCUnicastPkts                     : 46199
rxHCMulticastPkts                   : 383
txHCMulticastPkts                   : 9848
rxHCBroadcastPkts                   : 595
txHCBroadcastPkts                   : 7871
rxHCOctets                          : 14339916
txHCOctets                          : 13420831
rxHCPkt64Octets                     : 45325
rxHCPkt65to127Octets                : 1058
rxHCPkt128to255Octets               : 0
rxHCPkt256to511Octets               : 4705
rxHCPkt512to1023Octets              : 15916
rxHCPkt1024to1518Octets             : 0
rxHCPkt1519to1522Octets             : 0
rxHCPkt1519to2047Octets             : 0
rxHCPkt2048to4095Octets             : 0
rxHCPkt4096to9216Octets             : 0
txHCPkt64Octets                     : 6347
txHCPkt65to127Octets                : 21566
txHCPkt128to255Octets               : 27683
txHCPkt256to511Octets               : 5822
txHCPkt512to1023Octets              : 270
txHCPkt1024to1518Octets             : 2230
txHCPkt1519to1522Octets             : 0
txHCPkt1519to2047Octets             : 0
txHCPkt2048to4095Octets             : 0
txHCPkt4096to9216Octets             : 0

rxCRCErrors                         : 0
rxUndersizedPkts                    : 0
rxOversizedPkts                     : 0
rxFragmentPkts                      : 0
rxjabbers                           : 0
rxSymbolErrors                      : 0

txCollisions                        : 0
ifInErrors                          : 0
ifOutErrors                         : 0
ifInDiscards                        : 0
ifOutDiscards                       : 0
txCRC                               : 0

dot3StatsSingleColFrames            : 0
dot3StatsMultiColFrames             : 0
dot3StatsDeferredTransmisions       : 0
dot3StatsLateCollisions             : 0
dot3StatsExcessiveCollisions        : 0
dot3StatsFrameTooLongs              : 0

linkChange                          : 1

GA-MLxxTPoE+#
```

Display Parameters

Parameters	Description
rxHCTotalPkts	Receive Packet Counter. Incremented for each packet received (includes bad packets, all Unicast, Broadcast, Multicast Packets, and MAC control packets).
txHCTotalPkts	Transmit Packet Counter. Incremented for each packet transmitted (including bad packets, all Unicast, Broadcast, Multicast packets and MAC control packets).
rxHCUnicastPkts	Receive Unicast Packet Counter. Incremented for each good unicast packet received.
txHCUnicastPkts	Transmit Unicast Packet Counter. Incremented for each good unicast packet transmitted.
rxHCMulticastPkts	Receive Multicast Packet Counter. Incremented for each good Multicast packet received. (Excluding MAC control packets).
txHCMulticastPkts	Transmit Multicast Packet Counter. Incremented for each good Multicast packet transmitted. (Excluding MAC control frames).
rxHCBroadcastPkts	Receive Broadcast Packet Counter. Incremented for each good Broadcast packet received.
txHCBroadcastPkts	Transmit Broadcast Packet Counter. Incremented for each good Broadcast packet transmitted.
rxHCOctets	Receive Byte Counter. Incremented by the byte count of packets received, including bad packets. (Excluding framing bits but including FCS bytes). **Note:** For truncated packet, the counter only counts up to max-rcv-frame-size.
txHCOctets	Transmit Byte Counter. Incremented for the bytes of packets transmitted. (Excluding framing bits but including FCS bytes).
rxHCPkt64Octets	Receive 64 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 64 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt65to127Octets	Receive 65 to 127 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 65 to 127 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt128to255Octets	Receive 128 to 255 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 128 to 255 bytes in length inclusive (excluding framing bits but including FCS bytes).

Parameters	Description
rxHCPkt256to511Octets	Receive 256 to 511 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len /Type error) frame received which is 256 to 511 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt512to1023Octets	Receive 512 to 1023 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 512 to 1023 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt1024to1518Octets	Receive 1024 to 1518 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 1024 to 1518 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt1519to1522Octets	Receive 1519 to 1522 Byte Good VLAN Frame Counter. Incremented for each good VLAN (excludes FCS, Symbol, Truncated error) frame received which is 1519 to 1522 bytes in length inclusive (excluding framing bits but including FCS bytes). Counts both single and double tag frames.
rxHCPkt1519to2047Octets	Receive 1519 to 2047 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 1519 to 2047 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt2048to4095Octets	Receive 2048 to 4095 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 2048 to 4095 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt4096to9216Octets	Receive 4096 to 9216 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 4096 to 9216 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt9217to16383Octets	Receive 9217 to 16383 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 9217 to 16383 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt64Octets	Transmit 64 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 64 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt65to127Octets	Transmit 65 to 127 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 65 to 127 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt128to255Octets	Transmit 128 to 255 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 128 to 255 bytes in length inclusive (excluding framing bits but including FCS bytes).

Parameters	Description
txHCPkt256to511Octets	Transmit t 256 to 511 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 256 to 511 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt512to1023Octets	Transmit 512 to 1023 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 512 to 1023 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt1024to1518Octets	Transmit 1024 to 1518 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 1024 to 1518 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt1519to1522Octets	Transmit 1519 to 1522 Byte Good VLAN Frame Counter. Incremented for each good VLAN (excludes FCS and TX errors) frame transmitted which is 1519 to 1522 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt1519to2047Octets	Transmit 1519 to 2047 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 1519 to 2047 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt2048to4095Octets	Transmit 2048 to 4095 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 2048 to 4095 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt4096to9216Octets	Transmit 4096 to 9216 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 4096 to 9216 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt9217to16383Octets	Transmit 9217 to 16383 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 9217 to 16383 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxCRCErrors	Receive Error Frame Counter. Incremented for each packet received which is 64 to max-rcv-frame-size (or max-rcv-frame-size+4 for tagged frames) octets in length (excluding framing bits, but including FCS octets), but had either a bad FCS with an integral number of octets (FCS Error).
rxUndersizedPkts	Receive Undersize Frame Counter. Incremented for each packet received which is less than 64 bytes in length (excluding framing bits, but including FCS octets) and is otherwise well formed (contains a valid FCS).

Parameters	Description
rxOversizedPkts	Receive Oversized Frame Counter. Incremented for each packet received which is longer than 1518 bytes in length (excluding framing bits, but including FCS octets) and is otherwise well formed (contain a valid FCS). Note: Whether oversized frame could be counted is ASIC dependent. For GA-ML series, only when the max-rcv-frame-size is not less than 1518, increased for each untagged packet received which is larger than max-rcv-frame-size and lower than max-rcv-frame-size+4 in length (including the FCS bits and excluding the frame header) and have valid FCS value.
rxFragmentPkts	Receive Fragment Counter. Incremented for each packet received which is less than 64 bytes in length (excluding framing bits but including FCS octets) and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
rxJabbers	Receive Jabber Frame Counter. Incremented for each packet received which is longer than 1518 bytes in length (excluding framing bits, but including FCS octets), and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note: Whether rxJabbers could be counted is ASIC dependent. For GA-ML series, only when the max-rcv-frame-size is not less than 1518, increased for each untagged packet received which is larger than max-rcv-frame-size and lower than max-rcv-frame-size+4 in length (including the FCS bits and excluding the frame header) and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
rxSymbolErrors	Receive Code Error Frame Counter. Incremented for the count of times where there was an invalid data symbol when a valid carrier was present.
txCollisions	Transmit Total Collision Counter. Incremented by the total number of collisions experienced during the transmission.
ifInErrors	Received Error Packet Counter. Incremented for received packets which contained errors preventing them from being deliverable to a higher-layer protocol. The counter is the sum of dot3StatsAlignmentErrors, dot3StatsFCSErrors, dot3StatsFrameTooLongs, and dot3StatsInternalReceiveError.

Parameters	Description
ifOutErrors	Transmit Error Packet Counter. Incremented for outbound packets which could not be transmitted because of errors. The counter is the sum of dot3StatsSQETestErrors, dot3StatsLateCollisions, dot3StatsExcessiveCollisions, dot3StatsInternalMacTransmitErrors and dot3StatsCarrierSenseErrors.
ifInDiscards	Receive Discards Packet Counter. Incremented for packets received which are dropped due to any condition. Such as MTU drop, Buffer Full Drop, ACL Drop, Multicast Drop, VLAN Ingress Drop, Invalid IPv6, STP Drop, Storm and FDB Discard, and etc.
ifOutDiscards	Transmit Discards Packet Counter. Incremented for packets transmitted which are dropped due to any condition. Such as excessive transit delay discards, HOL drop, STP drop, MTU drop, VLAN drop, and etc.
txCRC	Transmit FCS Error Packet Counter. Incremented for each frame transmitted which does not pass the FCS check.
dot3StatsSingleColFrames	Transmit Single Collision Frame Counter. 10/100 mode only—incremented for each frame transmitted which experienced exactly one collision during transmission.
dot3StatsMultiColFrames	Transmit Multiple Collision Frame Counter. 10/100 mode only—incremented for each frame successfully transmitted for which transmission is inhibited by more than one collision.
dot3StatsDeferredTransmissions	Transmit Single Deferral Frame Counter. 10/100 mode only—incremented for each frame which was deferred on its first transmission attempt and did not experience any subsequence collisions during transmission.
dot3StatsLateCollisions	Transmit Late Collision Frame Counter. 10/100 mode only—incremented for each frame transmitted which experienced a late collision during a transmission attempt.
dot3StatsExcessiveCollisions	Transmit Excessive Collision Frame Counter. 10/100 mode only—incremented for each frame transmitted for which transmission fails due to excessive collisions.
dot3StatsFrameTooLongs	Receive Frame Too Long Counter. Incremented for each frame received which exceeds the max-rcv-frame-size.

3.1.6 show interfaces

This command is used to display the interface information.

Syntax

- **show interfaces** [*INTERFACE-ID* [**,** | **-**]]

Parameters

Parameters	Description
INTERFACE-ID	(Optional) Specifies that the interface can be a physical port, VLAN, loopback interface, or other.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

If no interface was specified, all existing interfaces will be displayed.

Example

This example shows how to display the VLAN interface information for interface VLAN 1.

```
GA-MLxxTPoE+#show interfaces vlan 1

vlan1 is enabled, Link status is up
  Interface type: VLAN
  MAC address: 00-50-40-xx-xx-xx


GA-MLxxTPoE+#
```

This example shows how to display the interface information for GigabitEthernet 1/0/1.

```
GA-MLxxTPoE+#show interfaces GigabitEthernet 1/0/1

GigabitEthernet 1/0/1 is enabled link status is up
  Interface type: 1000BASE-T
  Interface description:
  MAC Address: 00-50-40-xx-xx-xx
  Auto-duplex, auto-speed, auto-mdix
  Send flow-control: off, receive flow-control: off
  Send flow-control oper: off, receive flow-control oper: off
  Full-duplex, 1Gb/s
  Maximum transmit unit: 1518 bytes
  RX rate: 0 bits/sec, TX rate: 0 bits/sec
  RX bytes: 66544, TX bytes: 462219
  RX rate: 0 packets/sec, TX rate: 0 packets/sec
  RX packets: 509, TX packets: 3217
  RX multicast: 44, RX broadcast: 428
  RX CRC error: 0, RX undersize: 0
  RX oversize: 0, RX fragment: 0
  RX jabber: 0, RX dropped Pkts: 0
  RX MTU exceeded: 0
  TX CRC error: 0, TX excessive deferral: 0
  TX single collision: 0, TX excessive collision: 0
  TX late collision: 0, TX collision: 0


GA-MLxxTPoE+#
```

3.1.7 show interfaces counters

This command is used to display counters on specified interfaces.

Syntax

- **show interfaces [***INTERFACE-ID* **[, | -]] counters [errors]**

Parameters

Parameters	Description
INTERFACE-ID	(Optional) Specifies that the interface can be a physical port or VLAN interfaces. If no interface is specified, the counters on all interfaces will be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
errors	(Optional) Specifies to display the error counters.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command allows the user to display general, error or historical statistics counters for the specified or all interfaces.

Example

This example shows how to display switch port RX counters on GigabitEthernet1/0/1 to 1/0/2.

```
GA-MLxxTPoE+#show interfaces GigabitEthernet 1/0/1-2 counters

Port          InOctets /              InMcastPkts /
              InUcastPkts             InBcastPkts
------------- ----------------------- -----------------------
Gi1/0/1       42651                   43
              71                      474
Gi1/0/2       0                       0
              0                       0

Port          OutOctets /             OutMcastPkts /
              OutUcastPkts            OutBcastPkts
------------- ----------------------- -----------------------
Gi1/0/1       29789                   0
              61                      0
Gi1/0/2       0                       0
              0                       0

Total Entries:2


GA-MLxxTPoE+#
```

This example shows how to display switch ports error counters.

```
GA-MLxxTPoE+#show interfaces GigabitEthernet 1/0/1,1/0/3 counters errors

Port          Undersize /            Fcs-Err /
              Rcv-Err /              InDiscard /
              Xmit-Err               OutDiscard
------------- ---------------------- ----------------------
Gi1/0/1       0                      0
              0                      100
              0                      0
Gi1/0/3       0                      0
              0                      0
              0                      0

Port          Single-Col /           Excess-Col /
              Multi-Col /            Late-Col /
              DeferredTx             Symbol-Err
------------- ---------------------- ----------------------
Gi1/0/1       0                      0
              0                      0
              0                      0
Gi1/0/3       0                      0
              0                      0
              0                      0

Total Entries:2


GA-MLxxTPoE+#
```

Display Parameters

Parameters	Description
UnderSize	refer to the item “rxUndersizedPkts” in Display Parameters in the **show counters** command.
Rcv-Err	refer to the item “ifInErrors” in Display Parameters in the **show counters** command.
Xmit-Err	refer to the item “ifOutErrors” in Display Parameters in the **show counters** command.
Fcs-Err	refer to the item “dot3StatsFCSErrors” in Display Parameters in the **show counters** command.
InDiscard	refer to the item “ifInDiscards” in Display Parameters in the **show counters** command.
OutDiscard	refer to the item “ifOutDiscards” in Display Parameters in the **show counters** command.
Single-Col	refer to the item “dot3StatsSingleColFrames” in Display Parameters in the **show counters** command.
Multi-Col	refer to the item “dot3StatsMultiColFrames” in Display Parameters in the **show counters** command.
DeferredTx	refer to the item “txDelayExceededDiscards” in Display Parameters in the **show counters** command.

Parameters	Description
Excess-Col	refer to the item "dot3StatsExcessiveCollisions" in Display Parameters in the **show counters** command.
Late-Col	refer to the item "dot3StatsLateCollisions" in Display Parameters in the **show counters** command.
Symbol-Err	refer to the item "rxSymbolErrors" in Display Parameters in the **show counters** command.

3.1.8 show interfaces status

This command is used to display the Switch's port connection status.

Syntax

- **show interfaces** [*INTERFACE-ID* **[, | -]] status**

Parameters

Parameters	Description
INTERFACE-ID	(Optional) Specifies the interface ID. If no interface is specified, the connection status of all switch ports will be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command displays the Switch's port connection status.

Example

This example shows how to display the Switch's port connection status.

```
GA-MLxxTPoE+#show interfaces status

Port          Status        VLAN         Duplex  Speed          Type
------------- ------------- ------------ ------- -------------- -------------
Gi1/0/1       not-connected 1            auto    auto           1000BASE-T
Gi1/0/2       not-connected 3            auto    auto           1000BASE-T
Gi1/0/3       not-connected 1            auto    auto           1000BASE-T
Gi1/0/4       not-connected 1            auto    auto           1000BASE-T
Gi1/0/5       not-connected 1            auto    auto           1000BASE-T
Gi1/0/6       not-connected 1            auto    auto           1000BASE-T
Gi1/0/7       not-connected 1            auto    auto           1000BASE-T
Gi1/0/8       not-connected 1            auto    auto           1000BASE-T
Gi1/0/9(c)    not-connected 1            auto    auto           1000BASE-T
Gi1/0/9(f)    not-connected 1            auto    auto           1000BASE-X
Gi1/0/10(c)   not-connected 1            auto    auto           1000BASE-T
Gi1/0/10(f)   not-connected 1            auto    auto           1000BASE-X

Total Entries: 10

GA-MLxxTPoE+#
```

3.1.9 show interfaces utilization

This command is used to display the Switch's port utilization.

Syntax

- **show interfaces [***INTERFACE-ID* **[, | -]] utilization**

Parameters

Parameters	Description
INTERFACE-ID	(Optional) Specifies the interface ID. If no interface is specified, the utilization of all physical port interfaces will be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional)Specifies a range of interfaces. No space is allowed before or after the hyphen.
utilization	(Optional) Specifies to display the utilization information.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

The command allows the user not only to view the utilization for all interfaces or specified interfaces, but also to view the Switch historical CPU and Memory utilization.
A particular rate statistics of a port-channel is the sum of all physical member port interface rate for that port-channel. For example, physical port interfaces, GigabitEthernet1/0/1 to GigabitEthernet1/0/4, belong to the same port-channel, the RX rate (packets per second) of each port is 100, 200, 200,100. As a result, the CRC error packets of the port-channel is 600 packets per second.

Example

This example shows how to display the Switch's port utilization.

```
GA-MLxxTPoE+#show interfaces utilization

Port           TX packets/sec    RX packets/sec    Utilization
-------------  ----------------- ----------------- -----------
Gi1/0/1        0                 0                 0
Gi1/0/2        0                 0                 0
Gi1/0/3        0                 0                 0
Gi1/0/4        0                 0                 0
Gi1/0/5        0                 0                 0
Gi1/0/6        0                 0                 0
Gi1/0/7        0                 0                 0
Gi1/0/8        0                 0                 0
Gi1/0/9        0                 0                 0
Gi1/0/10       0                 0                 0
Gi1/0/11       0                 0                 0
Gi1/0/12       0                 0                 0
Gi1/0/13       0                 0                 0
Gi1/0/14       0                 0                 0
Gi1/0/15       0                 0                 0
Gi1/0/16       0                 0                 0
Gi1/0/17       0                 0                 0
Gi1/0/18       0                 0                 0
Gi1/0/19       0                 0                 0
Gi1/0/20       0                 0                 0
Gi1/0/21       0                 0                 0
--More--
```

3.1.10 show interfaces fiber_module

This command is used to display fiber module status information.

Syntax

- **show interfaces** [*INTERFACE-ID* [**,** | **-**]] **fiber_module**

Parameters

Parameters	Description
INTERFACE-ID	(Optional) Specifies the interface ID. If no interface is specified, the fiber module status information on all fiber module interfaces will be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
fiber_module	Specifies to display fiber module status information.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command displays fiber module status information.

Example

This example shows how to display fiber module status information.

```
GA-MLxxTPoE+#show interfaces GigabitEthernet 1/0/21 fiber_module

GigabitEthernet 1/0/21
 Interface Type: 1000BASE-X
 Laser Identifier: SFP
 Connector Type: LC
 Ethernet Compliance Code: 1000BASE-SX
 Encoding: 8B/10B
 Vendor Name: Panasonic
 Vendor OUI: 00:50:40
 Vendor PN: xxxxxx
 Vendor Rev: 0000
 Vendor SN: xxxxxxxxxxx
 Date Code: xxxxxx
 Received Power Measurements Type: Average Power
 Compatibility: Multi-Mode,1300Mbd, 850nm
 Transfer Distance:
   50/125 um OM2 fiber: 550m
   62.5/125 um OM1 fiber: 300m


GA-MLxxTPoE+#
```

3.1.11 show interfaces auto-negotiation

This command is used to display detailed auto-negotiation information of physical port interfaces.

Syntax

- **show interfaces** [*INTERFACE-ID* [**,** | **-**]] **auto-negotiation**

Parameters

Parameters	Description
INTERFACE-ID	(Optional) Specifies the interface ID. If no interface is specified, the auto-negotiation information on all physical port interfaces will be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
auto-negotiation	Specifies to display detailed auto-negotiation information.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command displays the auto-negotiation information.

Example

This example shows how to display auto-negotiation information.

```
GA-MLxxTPoE+#show interfaces GigabitEthernet 1/0/1 auto-negotiation

GigabitEthernet 1/0/1
 Auto Negotiation: Enabled

 Remote Signaling: Not detected
 Configure Status: Complete
 Capability Bits: 10M_Full, 100M_Full, 1000M_Full
 Capability Advertised Bits: 10M_Full, 100M_Full, 1000M_Full
 Capability Received Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full, 1000M_Half, 1000M_Full
 RemoteFaultAdvertised: Disabled
 RemoteFaultReceived: NoError


GA-MLxxTPoE+#
```

3.1.12 show interfaces description

This command is used to display the description and link status of interfaces.

Syntax

- **show interfaces** [*INTERFACE-ID* [**,** | **-**]] **description**

Parameters

Parameters	Description
INTERFACE-ID	(Optional) Specifies the interface ID. If no interface is specified, then information related to all interfaces will be displayed.

Parameters	Description
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
description	Specifies to display the description and link status of interfaces.

Default

None

Command Mode

User/Privileged EXEC Mode
Any Configuration Mode

Command Default Level

Level: 1

Usage Guideline

This command displays the description and link status of interfaces.

Example

This example shows how to display the description and link status of interfaces.

```
GA-MLxxTPoE+#show interfaces description

 Interface             Status    Administrative  Description
 --------------------  --------  --------------  ------------------------------
 Gi1/0/1               up        enabled
 Gi1/0/2               down      enabled
 Gi1/0/3               down      enabled
 Gi1/0/4               down      enabled
 Gi1/0/5               down      enabled
 Gi1/0/6               down      enabled
 Gi1/0/7               down      enabled
 Gi1/0/8               down      enabled
 Gi1/0/9               down      enabled
 Gi1/0/10              down      enabled         Pysical Port 10
 Gi1/0/11              down      enabled
 Gi1/0/12              down      enabled
 Gi1/0/13              down      enabled
 Gi1/0/14              down      enabled
 Gi1/0/15              down      enabled
 Gi1/0/16              down      enabled
 Gi1/0/17              down      enabled
 Gi1/0/18              down      enabled
 Gi1/0/19              down      enabled
 Gi1/0/20              down      enabled
 Gi1/0/21              down      enabled
--More--
```

3.1.13 shutdown

This command is used to disable an interface. Use the **no** form of this command to enable an interface.

Syntax

- **shutdown**
- **no shutdown**

Parameters

None

Default

By default, this option is **no shutdown**.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The Physical port, loopback, VLAN, tunnel, and management interfaces are valid for this configuration. This command is also configurable for port channel member ports.
The command will cause the port to enter the disabled state. Under the disabled state, the port will not be able to receive or transmit any packets. Using the **no shutdown** command will put the port back into the enabled state. When a port is shut down, the link status will also be turned off.

Example

This example shows how to enter the shutdown command to disable the port state of interface port 1/0/1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface GigabitEthernet 1/0/1
GA-MLxxTPoE+(config-if)#shutdown
GA-MLxxTPoE+(config-if)#
```

3.2 Switch Port Commands

3.2.1 duplex

This command is used to configure the physical port interface's duplex setting. Use the **no** form of this command to revert to the default settings.

Syntax

- **duplex {full | auto | harf} [rj45 | sfp]**
- **no duplex [rj45 | sfp]**

Parameters

Parameters	Description
full	Specifies that the port operates in the full-duplex mode.
auto	Specifies that the port's duplex mode will be determined by auto-negotiation.
half	Specifies that the port operates in the half-duplex mode
rj45	(Optional) Specifies to configure the duplex for RJ45 media. For combo ports, if RJ45 or SFP is not specified, RJ45 is implied.
sfp	(Optional) Specifies to configure the duplex for SFP media.

Default

The duplex mode will be set as automatic for 100BASE-TX and 1000BASE-T interfaces.
The duplex mode will be set as full for 100BASE-FX and 1000BASE-SX/LX interfaces.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

100BASE-FX is always set at the speed of 10 Mbps and full-duplex. 1000BASE-SX/LX is always set at the speed of 100 Mbps and full-duplex.
For 100BASE-FX and 1000BASE-SX/LX modules, this command cannot take effect.
Auto-negotiation will be enabled if either the speed parameter is set to auto or the duplex parameter is set to auto if the speed parameter is set to auto and the duplex parameter is set to the fixed mode only the speed will be negotiated. The advertised capability will be configured to the duplex mode combined with all the possible speeds. If the speed is to set to a fixed speed and duplex is set to auto, only the duplex mode is negotiated.

Example

This example shows how to configure the GigabitEthernet1/0/1 to operate at a forced speed of 100Mbits and specifies that the duplex mode should be set to auto-negotiated.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#speed 100
GA-MLxxTPoE+(config-if)#duplex auto
GA-MLxxTPoE+(config-if)#
```

3.2.2 flowcontrol

This command is used to configure the flow control capability of the port interface. Use the **no** form of this command to revert to the default setting.

Syntax

- **flowcontrol {on | off}**
- **no flowcontrol**

Parameters

Parameters	Description
on	Specifies to enable a port to send PAUSE frames or process PAUSE frames from remote ports.
off	Specifies to disable the ability for a port to send or receive PAUSE frames.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command can only assure that the flow control capability has been configured in the Switch software and not guarantee the actual hardware operation. The actual hardware operation may be different to the settings that have been configured on the Switch because the flow control capability is determined by both the local port/device and the device connected at the other end of the link, not just by the local device.
If the speed is set to the forced mode, the final flow control setting will be determined by the configured flow control setting. If the speed is set to the auto mode, the final flow control setting will be based on the negotiated result between the local side setting and the partner side setting. The configured flow control setting here is the local side setting.

Example

This example shows how to enable the flow control on GigabitEthernet 1/0/1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#flowcontrol on
GA-MLxxTPoE+(config-if)#
```

3.2.3 media-type

This command is used to configure the media of a combo port that is selected for connection. Use the **no** form of this command to revert to the default settings.

Syntax

- **media-type {auto-select | rj45 | sfp}**
- **no media-type**

Parameters

Parameters	Description
auto-select	Specifies that the media is selected based on the user's connection.
rj45	Specifies to use RJ45 media for the connection, and SFP is disabled.
sfp	Specifies to use SFP media for the connection, and RJ45 is disabled.

Default

By default, this option is auto-select.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for the combo ports.

Example

This example shows how to configure the media type for interface GigabitEthernet 1/0/21 to sfp.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/21
GA-MLxxTPoE+(config-if)#media-type sfp
GA-MLxxTPoE+(config-if)#
```

3.2.4 mdix

This command is used to configure the port Media-Dependent Interface Crossover (MDIX) state. Use the no form of this command to revert to the default setting.

Syntax

- mdix {auto | normal | cross}

- no mdix

Parameters

Parameters	Description
auto	Specifies to set the port interface's MDIX state to the auto-MDIX mode.
normal	Specifies to force the port interface's MDIX state to the normal mode.
cross	Specifies to force the port interface's MDIX state to the cross mode.

Default

down link ports (no combo ports) : auto
up link ports (combo ports) : disabled

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command cannot be applied to a port when the medium of the port interface is fiber.

Example

This example shows how to configure the MDIX state of interface GigabitEthernet 1/0/1 to auto:

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#mdix auto
GA-MLxxTPoE+(config-if)#
```

3.2.5 speed

This command is used to configure the physical port interface's speed settings. Use the no form of this command to revert to the default setting.

Syntax

- **speed {10 | 100 | 1000 [master | slave] | auto [*SPEED-LIST*]} [rj45 | sfp]**
- no speed [rj45 | sfp]

Parameters

Parameters	Description
10	Specifies to force the speed to 10Mbps.
100	Specifies to force the speed to 100Mbps.
1000	Specifies that for copper ports, it forces the speed to 1000Mbps and the user must manually set that the port operates as master or slave. Specifies that for fiber ports (1000BASE-SX/LX), the port will disable the auto-negotiation.
master | slave	Specifies the port operates as master or slave timing. This parameter is only applicable to 1000BASE-T connections.
auto	Specifies that for copper ports, it specifies to determine the speed and flow control via auto-negotiation with its link partner. Specifies that for fiber ports (1000BASE-SX/LX), it enables the auto-negotiation option. Auto-negotiation will start to negotiate the clock and flow control with its link partner.
SPEED-LIST	(Optional) Specifies a list of speeds that the Switch will only auto-negotiate to. The speed can be 1000. Use a comma (,) to separate multiple speeds. If the speed list is not specified, all speed will be advertised.
rj45	(Optional) Specifies to configure speed for RJ45 media. For combo ports, if RJ45 or SFP/SFP+ is not specified, RJ45 is used.
sfp	(Optional) Specifies to configure speed for SFP/SFP+ media.

Default

The speed is automatic for 100BASE-TX and 1000BASE-T interfaces.
The speed is fixed to 1000Mbps for 1000BASE-FX interfaces.
The speed is fixed to 1000Mbps for 1000BASE-SX/LX interfaces.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

If the specified speed is not supported by the hardware, error messages will be returned. For the 100BASE-FX modules, the speed is always fixed at 100Mbps, full duplex, and no-negotiation. No command can change the settings. For the 1000BASE-SX/LX modules, the speed is always fixed to 1000Mbps and full duplex, and only the **speed 1000** and **speed auto** commands are valid. For a 1000BASE-T connection, if the speed is specified to 1000Mbps, the port must be configured as master or slave.
Auto-negotiation will be enabled if either the speed parameter is set to **auto**, or the duplex parameter is set to **auto**. If the speed parameter is set to auto, and the duplex parameter is set to the fixed mode. Only the speed will be negotiated. The advertised capability will be configured to the duplex mode combined with all the possible speeds. If the speed is to set to a fixed speed and duplex is set to auto, only the duplex mode is negotiated.

Example

This example shows how to configure GigabitEthernet 1/0/1 to only auto-negotiate to 10Mbps or 100Mbps.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#speed auto 10,100
GA-MLxxTPoE+(config-if)#
```

3.3 Jumbo Frame Commands

3.3.1 max-rcv-frame-size

This command is used to configure the maximum Ethernet frame size allowed. Use the **no** form of this command to revert to the default setting.

Syntax

- **max-rcv-frame-size** *BYTES*
- **no max-rcv-frame-size**

Parameters

Parameters	Description
BYTES	Specifies the maximum Ethernet frame size allowed. The range is from 64 to 9216 bytes.

Default

By default, this value is 1518 bytes.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is available for physical ports configuration. Oversize frames will be dropped and checks are carried out on ingress ports. Use this command to transfer large frames or jumbo frames through the Switch to optimize server-to-server performance.

Example

This example shows how to configure the maximum received Ethernet frame size to be 6000 bytes on port 1/0/3.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/3
GA-MLxxTPoE+(config-if)#max-rcv-frame-size 6000
GA-MLxxTPoE+(config-if)#
```

3.4 Power Saving Commands

3.4.1 line power-saving

This command is used to configure the power-saving mode for ports
The power saving mode is our unique function for automatically detecting the port connection status and minimizing power consumption if not connected. This Switching Hub supports two modes: the Half mode for giving priority to connectivity with other device, and the Full mode for minimizing power consumption.

Syntax

- **line power-saving {disable | full | half}**

Parameters

Parameters	Description
disable	Specifies to disable the power saving function.
half	Specifies to fully enable the power saving function.
full	Specifies to enable the power saving function between disable and full.

Default

By default, this option is disable.

Command Mode

Interface Configuration Mode.

Command Default Level

Level：12

Usage Guideline

This command is used to enable or disable the power saving function.

Example

This example shows how to enable power saving on Gigabit Ethernet ports 1/0/1-2.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface range gi1/0/1-2
GA-MLxxTPoE+(config-if-range)#line power-saving full
GA-MLxxTPoE+(config-if-range)#
```

3.4.2 line eee

This command is used to configure the Energy-Efficient Ethernet (EEE) function for specified ports. Use the no form of this command to revert to the default setting. The EEE power-saving mode saves power consumption while a link is up when there is low utilization of packet traffic.

Syntax

line eee

- **no line eee**

Parameters

None

Default

disabled

Command Mode

Interface Configuration Mode

Command Default Level

Level：12

Usage Guideline

This command is only available for down link ports (no combo ports).
The physical interface will enter into a Low Power Idle (LPI) mode when there is no data to be transmitted. In order to use EEE, the opposite port must also be EEE compliant.

Example

This example shows how to enable the EEE power saving function.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#line eee
GA-MLxxTPoE+(config-if)#
```

3.4.3 show line configuration

This command is used to display the line configuration information.

Syntax

- **show line configuration**

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level：1

Usage Guideline

This command is used to display the line configuration information.

Example

This example shows how to display the line configuration information.

```
GA-MLxxTPoE+#show line configuration

Interface    Link     Type      Mode              Power-saving  EEE
---------    -------- --------- ----------------- ------------- ---------
Gi1/0/1      Up       1000T     Auto(100F)        Full          Enabled
Gi1/0/2      Down     1000T     Auto              Full          Enabled
Gi1/0/3      Up       1000T     Auto(100F)        Disabled      Enabled
Gi1/0/4      Down     1000T     Auto              Disabled      Enabled
Gi1/0/5      Down     1000T     Auto              Disabled      Enabled
Gi1/0/6      Down     1000T     Auto              Disabled      Enabled
Gi1/0/7      Down     1000T     Auto              Disabled      Enabled
Gi1/0/8      Down     1000T     Auto              Disabled      Enabled
Gi1/0/9      Down     1000T     Auto              Disabled      Enabled
Gi1/0/10     Down     1000T     Auto              Disabled      Enabled
Gi1/0/11     Down     1000T     Auto              Disabled      Enabled
Gi1/0/12     Down     1000T     Auto              Disabled      Enabled
Gi1/0/13     Down     1000T     Auto              Disabled      Enabled
Gi1/0/14     Down     1000T     Auto              Disabled      Enabled
Gi1/0/15     Down     1000T     Auto              Disabled      Enabled
Gi1/0/16     Down     1000T     Auto              Disabled      Enabled
Gi1/0/17     Down     1000T     Auto              Disabled      Enabled
Gi1/0/18     Down     1000T     Auto              Disabled      Enabled
Gi1/0/19     Down     1000T     Auto              Disabled      Enabled
Gi1/0/20     Down     1000T     Auto              Disabled      Enabled
Gi1/0/21     Down     1000T     Auto              Disabled      Enabled
--More--
```

3.5 Error Disable Commands

3.5.1 errdisable recovery

This command is used to enable the error recovery for causes and to configure the recovery interval. Use the **no** form of this command to disable the auto-recovery option or to revert to the default setting for causes.

Syntax

- **errdisable recovery cause {all | psecure-violation | storm-control | bpdu-protect | arp-rate | dhcp-rate | l2pt-guard} [interval** *SECONDS*]
- **no errdisable recovery cause {all | psecure-violation | storm-control | bpdu-protect | arp-rate | dhcp-rate | l2pt-guard} [interval]**

Parameters

Parameters	Description
all	Specifies to enable the auto-recovery option for all causes.
arp-rate	Specifies to enable the auto-recovery option for an error port caused by ARP rate limiting.
bpdu-protect	Specifies to enable the auto-recovery option for an error port caused by BPDU guard.
dhcp-rate	Specifies to enable the auto-recovery option for an error port caused by DHCP rate limiting.
l2pt-guard	Specifies to enable the auto-recovery option for an error port caused by L2PT guard.
psecure-violation	Specifies to enable the auto-recovery option for an error port caused by port security violation.
storm-control	Specifies to enable the auto-recovery option for an error port caused by storm control.
interval *SECONDS*	(Optional) Specifies the time, in seconds, to recover the port from the error state caused by the specified module. The valid value is 5 to 86400. The default value is 300 seconds.

Default

Auto-recovery is disabled for all causes.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

A port can be put in an error disabled state by causes such as port security violations, storm control and so on. When a port enters the error disabled state, the port is shutdown although the setting running the configuration remains in the no shutdown state.
There are two ways to recover an error disabled port. Administrators can use the **errdisable recovery cause** command to enable the auto-recovery of error ports disabled by each cause. Alternatively, administrators can manually recover the port by entering the **shutdown** command first and then the **no shutdown** command for the port.

Example

This example shows how to set the recovery timer to 200 seconds for port security violation.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# errdisable recovery cause psecure-violation interval 200
GA-MLxxTPoE+(config)#
```

This example shows how to enable the auto-recovery option for port security violations.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# errdisable recovery cause psecure-violation
GA-MLxxTPoE+(config)#
```

3.5.2 show errdisable recovery

This command is used to display the error-disable recovery timer related settings.

Syntax

- **show errdisable recovery**

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to verify the settings of the error disable recovery timer.

Example

This example shows how to display the settings of the error disable recovery timer.

```
GA-MLxxTPoE+# show errdisable recovery

ErrDisable Cause                      State          Interval
------------------------------------  -----------    -------------
Port Security                         enabled        120 seconds
Storm Control                         enabled        120 seconds
BPDU Attack Protection                disabled       120 seconds
Dynamic ARP Inspection                enabled        120 seconds
DHCP Snooping                         enabled        120 seconds
L2pt-guard                            disabled       300 seconds
Unidirectional Link Detection         disabled       300 seconds

Interfaces that will be recovered at the next timeout:

Interface    ErrDisable Cause                       Time left(sec)
---------    ------------------------------------   --------------
Gi1/0/7      BPDU Attack Protection                 infinite

GA-MLxxTPoE+#
```

3.6 Port Security Commands

3.6.1 clear port-security

This command is used to delete the auto-learned secured MAC addresses.

Syntax

- **clear port-security** {**all** | {**address** *MAC-ADDR* | **interface** *INTERFACE-ID* [**,** | **-**]} [**vlan** *VLAN-ID*]}

Parameters

Parameters	Description
all	Specifies to delete all auto-learned secured entries.
address *MAC-ADDR*	Specifies to delete the specified auto -learned secured entry based on the MAC address entered.
interface *INTERFACE-ID*	Specifies to delete all auto-learned secured entries on the specified physical interface.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
vlan *VLAN-ID*	Specifies to delete the auto-learned secured entry learned with the specified VLAN.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

This command clears auto-learned secured entries, either dynamic or permanent.

Example

This example shows how to remove a specific secure address from the MAC address table.

```
GA-MLxxTPoE+# clear port-security address 0050.4070.0007
GA-MLxxTPoE+#
```

3.6.2 show port-security

This command is used to display the current port security settings.

Syntax

- **show port-security** [[**interface** *INTERFACE-ID* [**,** | **-**]] [**address**] | **vlan** *VLAN-ID* [**,** | **-**]]

Parameters

Parameters	Description
interface *INTEFACE-ID*	(Optional) Specifies the ID of the interface to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
address	(Optional) Specifies to display all the secure MAC addresses, including both configured and learned entries.
vlan *VLAN-ID*	(Optional) Specifies to display port security settings for the VLAN.
.	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command is used to display the current port security settings.

Example

This example shows how to display the port security settings of interfaces GigabitEthernet1/0/1 to 1/0/3.

```
GA-MLxxTPoE+#show port-security interface gi 1/0/1-3

 D:Delete-on-Timeout    P:Permanent
 Interface    Max  Curr   Violation    Violation   Security  Admin   Current
 No.          No.   No.     Act.       Count           Mode  State   State
 ------------ ----- ----- -------- -------------------- -- -------- ------------
 Gi1/0/1      32    0     Protect  -                    D  Disabled -
 Gi1/0/2      32    0     Shutdown 0                    D  Enabled  Err-disabled
 Gi1/0/3      32    0     Shutdown 0                    P  Disabled -

GA-MLxxTPoE+#
```

3.6.3 snmp-server enable traps port-security

This command is used to enable the sending of SNMP notifications for port security address violations. Use the **no** form of this command to disable the sending of SNMP notifications.

Syntax

- **snmp-server enable traps port-security [trap-rate** *TRAP-RATE*]
- **no snmp-server enable traps port-security [trap-rate]**

Parameters

Parameters	Description
trap-rate *TRAP-RATE*	(Optional) Specifies the number of traps to send per second. The range is from 0 to 1000. The default value of 31 indicates that an SNMP trap is to be generated for every security violation.

Default

By default, this feature is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to enable or disable the sending of SNMP notifications for port security address violations.

Example

This example shows how to enable the sending of traps for port security address violations and set the number of traps per second to 3.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server enable traps port-security
GA-MLxxTPoE+(config)# snmp-server enable traps port-security trap-rate 3
GA-MLxxTPoE+(config)#
```

3.6.4 switchport port-security

This command is used to configure the port security settings to restrict the number of users that are allowed to gain access rights to a port. Use the **no** form of this command to disable port security or to delete a secure MAC address.

Syntax

- **switchport port-security** [**maximum** *VALUE* | **violation** {**protect** | **restrict** | **shutdown**} | **mode** {**permanent** | **delete-on-timeout**} | **mac-address** [**permanent**] *MAC-ADDRESS* [**vlan** *VLAN-ID*]]
- **no switchport port-security** [**maximum** | **violation** | **mode** | **mac-address** [**permanent**] *MAC-ADDRESS* [**vlan** *VLAN-ID*]]

Parameters

Parameters	Description
maximum *VALUE*	(Optional) Specifies to set the maximum number of secure MAC addresses allowed. If not specified, the default value is 32. The valid range is from 1 to 3328.
protect	(Optional) Specifies to drop all packets from the insecure hosts at the port-security process level, but does not increment the security-violation count.
restrict	(Optional) Specifies to drop all packets from the insecure hosts at the port-security process level and increments the security-violation count and record the system log.
shutdown	(Optional) Specifies to shut down the port if there is a security violation and record the system log.
permanent	(Optional) Specifies that under this mode, all learned MAC addresses will not be purged out unless the user manually deletes those entries.
delete-on-timeout	(Optional) Specifies that under this mode, all learned MAC addresses will be purged out when an entry is aged out or when the user manually deletes these entries.
mac-address *MAC-ADDRESS*	(Optional) Specifies to add a secure MAC address to gain port access rights.
permanent	(Optional) Specifies to set the secure permanent configured MAC address of the port. This entry is same as the one learnt under the permanent mode.
vlan *VLAN-ID*	(Optional) Specifies a VLAN. If no VLAN is specified, the MAC address will be set with a PVID.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

When port security is enabled, if the port mode is configured as **delete-on-timeout**, the port will automatically learn the dynamic secured entry which will be timed out. These entries will be aged out based on the setting specified by the **switchport port-security aging** command. If the port mode is permanent, the port will automatically learn permanent secured entries which will not be timed out. The auto-learned permanent secured entry will be stored in the running configuration.
As the port mode-security state is changed, the violation counts will be cleared, and the auto-permanent entries will be converted to corresponding dynamic entries. As the port-security state is changed to disabled, the auto-learned secured entries, either dynamic or permanent with its violation counts are cleared. As the related VLAN configuration is changed, the auto-learned dynamic secured entries are cleared.
Permanent secured entry will be kept in the running configuration and can be stored to the NVRAM by using the **copy** command. The user configured secure MAC addresses are counted in the maximum number of MAC addresses on a port.
As a permanent secured entry of a port security enabled port, the MAC address cannot be moved to another port.
When the maximum setting is changed, the learned address will remain unchanged when the maximum number increases. If the maximum number is changed to a lower value which is lower than the existing entry number, the command is rejected.
A port-security enabled port has the following restrictions.

- The port security function cannot be enabled simultaneously with 802.1X, MAC (MAC-based Access Control), WAC and IMPB, that provides more advanced security capabilities.
- If a port is specified as the destination port for the mirroring function, the port security function cannot be enabled.
- If the port is a link aggregation member port, the port security function cannot be enabled.

When the maximum number of secured users is exceeded, one of the following actions can occur:

- **Protect** - When the number of port secure MAC addresses reaches the maximum number of users that is allowed on the port, the packets with the unknown source address is dropped until some secured entry is removed to release the space.
- **Restrict** - A port security violation restricts data and causes the security violation counter to increment.
- **Shutdown** - The interface is disabled, based on errors, when a security violation occurs.

Example

This example shows how to configure the port security mode to be permanent, specifying that a maximum of 5 secure MAC addresses are allowed on the port.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# switchport port-security mode permanent
GA-MLxxTPoE+(config-if)# switchport port-security maximum 5
GA-MLxxTPoE+(config-if)#
```

This example shows how to manually add the secure MAC addresses 00-00-12-34-56-78 with VID 5 at GigabitEthernet1/0/1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#switchport port-security mac-address 00-00-12-34-56-78 vlan
5
GA-MLxxTPoE+(config-if)#
```

This example shows how to configure the Switch to drop all packets from the insecure hosts at the port-security process level and increment the security violation counter if a security violation is detected.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# switchport port-security violation restrict
GA-MLxxTPoE+(config-if)#
```

3.6.5 switchport port-security aging

This command is used to configure the aging time for auto-learned dynamic secure addresses on an interface. Use the **no** form of this command to revert to the default setting.

Syntax

- **switchport port-security aging {time** *MINUTES* **| type {absolute | inactivity}}**
- **no switchport port-security aging {time | type}**

Parameters

Parameters	Description
time *MINUTES*	Specifies the aging time for the auto-learned dynamic secured address on this port. Its range is from 1 to 1440 in minutes.
type	Specifies to set the aging type.

Parameters	Description
absolute	Specifies to set absolute aging type. All the secure addresses on this port age out exactly after the time specified and is removed from the secure address list. This is the default type.
inactivity	Specifies to set the inactivity aging type. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

Default

By default, the port security aging feature is disabled.
The default time is 0 minutes.
The default aging type is **absolute**.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to disable the ageing or set the ageing time for auto-learned dynamic secured entries. In order for the inactivity setting to take effect, the FDB table ageing function must be enabled.

Example

This example shows how to apply the aging time for automatically learned secure MAC addresses for GigabitEthernet1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# switchport port-security aging time 1
GA-MLxxTPoE+(config-if)#
```

This example shows how to configure the port security aging time type for GigabitEthernet1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# switchport port-security aging type inactivity
GA-MLxxTPoE+(config-if)#
```

3.6.6 port-security limit

This command is used to configure the maximum secure MAC address number on the system or on the specified VLAN. Use the **no** form of this command to revert to the default setting.

Syntax

- **port-security limit {global | vlan** *VLAN-ID* **[, | -]}** *VALUE*
- **no port-security limit {global | vlan** *VLAN-ID* **[, | -]}**

Parameters

Parameters	Description
global	Specifies that this setting will be applied to the system.
vlan *VLAN-ID*	Specifies the VLAN ID that will be used.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.
VALUE	Specifies the maximum number of port security entries that can be learned on the system or specified VLAN. The range is from 1 to 3328. If the setting is smaller than the number of current learned entries, the command will be rejected.

Default

By default, this option is no limit.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to set the limit on the port security entry number which can be learned on a system or on VLANs.

Example

This example shows how to configure the maximum secure MAC address number for the system.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# port-security limit global 100
GA-MLxxTPoE+(config)#
```

3.7 PoE (Power over Ethernet)

3.7.1 peth shutdown

The **peth shutdown** command is used to configure the stop of PoE power supply. Use the **no** form of this command to start the stopped PoE power supply.

Syntax

- **peth shutdown**
- **no peth shutdown**

Parameters

N/A

Default

By default, the stoppage for the PoE power-supply is disabled. The PoE power-supply is enabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to turn OFF/ON the PoE power supply on the interface. From the command input to the actual execution of power supply OFF or ON, it may take approximately 6 seconds.

Example

This example shows how to turn OFF the PoE power supply on port 1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#peth shutdown
```

3.7.2 peth limit

The **peth limit** command is used to configure the upper limit of PoE feeding power.

Syntax

- **peth limit** [auto | *power*]

Parameters

Parameter	Description
auto	Specifies the limit value according to the class of the power supply terminal.
power	Specifies the limit of feeding power statically. The set range is from 200 mW to 30000 mW (in 200 mW unit). [PN260496] The set range is from 200 mW to 95000 mW (in 200 mW unit).

Default

The default is auto.

Command Mode

Interface Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to configure the upper limit of PoE feeding power on the interface.

Example

This example shows how to configure the power supply limit of port 1 to 7000 mW.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#peth limit 7000
```

3.7.3 peth power-delivery delay-time

Use the command of **peth power-delivery delay-time** to configure the delayed time to start the PoE power-supply between interfaces. To disable the delayed time for starting the power-supply, use no form of the command.

Syntax

- **peth power-delivery delay-time** *delay time*
- **no peth power-delivery delay-time**

Parameters

Parameter	Description
delay time	This parameter configures the value with seconds to delay the starting time of the PoE power-supply of each interface; the range is from 0.1 to 10.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The power-supply may not start on the power-receiving device (or equipment), which can receive the power, including two ports. (However, this event does not occur regularly; it rarely occurs.) In that case, use this command to configure the delayed time for starting the PoE power-supply between interfaces. The recommendation value is 1.5 seconds.

Example

The following example describes how to set the delayed time (for starting the power-supply for each port) to 1.5 seconds.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#peth power-delivery delay-time 1.5
```

3.7.4 peth priority

The **peth priority** command is used to configure the priority of PoE power supply.

Syntax

- **peth limit** [low | high | critical]

Parameters

Parameter	Description
critical	Configure the priority as the highest.
high	Configure the priority as high.
low	Configure the priority as low.

Default

The default is low.

Command Mode

Interface Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to configure the power supply priority on the interface.

Example

This example shows how to configure the power supply priority of port 1 as the highest.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#peth priority critical
```

3.7.5 peth usage-threshold

The **usage-threshold** command is used to configure the threshold value which performs the trap notification according to the PoE power supply usage.

Syntax

- **peth usage-threshold** percent

Parameters

Parameter	Description
percent	Specifies the threshold value to compare with the measured electrify as a percentage (range: 1 to 99).

Default

The default threshold value is 50%.

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to configure the threshold value that performs the trap notification according to the PoE power supply usage.

Example

This example shows how to configure the threshold value of the trap notification of PoE power supply to 90%.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#peth usage-threshold 90
```

3.7.6 peth disconnection-method

The **peth disconnection-method** command is used to configure the power supply method when the feeding power exceeded the Power Budget.

Syntax

- **peth disconnection-method** [*next-port* | *low-priority*]

Parameters

Parameter	Description
next-port	Stops the power supply of the port which was connected right before the Power Budget was exceeded.
low-priority	Stops the power supply to the lowest priority port. When there are several ports of the same priority, the power supply to a port with the higher number will be stopped.

Default

The default value is *next-port*.

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to configure the power supply method when the feeding power exceeded the Power Budget.

Example

This example shows how to configure to stop the power supply of a port with the lowest priority.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#peth disconnection-method low-priority
```

3.7.7 snmp-server enable traps poe

The **snmp-server enable traps poe** command is used to configure the PoE power supply trap. Use the **no** form of this command to disable the trap.

Syntax

- **snmp-server enable traps poe**
- **no snmp-server enable traps poe**

Parameters

N/A

Default

The default is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to configure the PoE power supply trap.

Example

This example shows how to turn OFF the PoE power supply of port 1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#snmp-server enable traps poe
```

3.7.8 show peth-port

To display the information of the PoE power supply of all interfaces, use the **show peth-port** command.

Syntax

- **show peth-port**

Parameters

Parameter	Description
detail	[PN260496] (option)Display detailed information.

Default

N/A

Command Mode

Privileged Mode

Command Default Level

Level:1

Usage Guideline

This command is used to display the information of all ports.

Example

This example shows how to display the information of PoE power supply of all ports.

```
GA-MLxxTPoE+#show peth-port
 No. Admin Sche. Status Layer Class Prio.   Limit(mW)  Pow.(mW) Vol.(V) Cur.(mA)
 --- ----- ----- ------ ----- ----- ------ ----------- -------- ------- --------
  1   Up    -     NotPwr   -     -   Crit.         7000        0       0        0
  2   Up    -     Pwr      1     2   Low     7000(Auto)     2000      54       38
  3   Up    -     NotPwr   -     -   Low           Auto        0       0        0
  4   Up    -     NotPwr   -     -   Low           Auto        0       0        0
GA-MLxxTPoE+#
```

3.7.9 show peth power delay-time

Use the command of **show peth power delay-time** to display the delayed time for starting the PoE power-supply.

Syntax

- **show peth power delay-time**

Parameter

None

Default

None

Command Mode

Privilege Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display the delayed time for starting the PoE power-supply.

Example

The following example describes how to display the delayed time for starting the PoE power-supply.

```
GA-MLxxTPoE+#show peth power-delivery delay-time
PoE power delivery delay time: 1.5 seconds
GA-MLxxTPoE+#
```

3.7.10 show peth-conf

To display the global configuration of PoE power supply, use the **show peth-conf** command.

Syntax

- **show peth-conf**

Parameters

N/A

Default

N/A

Command Mode

Privileged Mode

Command Default Level

Level:1

Usage Guideline

This command is used to display the global configuration of PoE power supply.

Example

This example shows how to display the global configuration of PoE power supply.

```
GA-MLxxTPoE+#show peth-conf
 Fan Speed :                              High
 Power Budget :                           120W
 Power Consumption :                      2W
 Power Usage Threshold For Sending Trap:  50 %
 Power Management Method :  Deny next port connection, regardless of priority

GA-MLxxTPoE+#
```

3.8 PoE Scheduler

3.8.1 peth schedule enable (Global status)

This command is used to enable or disable the global configuration of PoE scheduler function. Use the **no** form of this command to disable it.

Syntax

- **peth schedule enable**
- **no peth schedule enable**

Parameters

N/A

Default

The default is enabled.

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guidelines

This command is used to enable or disable the global configuration of PoE scheduler function.

Example

This example shows how to enable the global configuration of PoE scheduler function.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#peth schedule enable
```

3.8.2 peth schedule enable (Schedule status)

This command is used to enable or disable the status settings of each PoE schedule. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth schedule** SCHEDULE-ID { **enable** | **disable** }

Parameters

Parameter	Description
SCHEDULE-ID	Specifies the PoE schedule ID to configure the PoE schedule status. The range is from 1 to 65535.
enable	Enables the PoE schedule status.
disable	Disables the PoE schedule status.

Default

N/A

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guidelines

This command is used to enable or disable the status settings of each PoE schedule.

Example

This example shows how to enable the status of PoE schedule 1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#peth schedule 1 enable
GA-MLxxTPoE+(config)#
```

3.8.3 peth schedule monthly

This command is used to configure the PoE schedule which is performed monthly. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth schedule** SCHEDULE-ID **name** SCHEDULE-NAME **monthly date** SCHEDULE-DATE **time** SCHEDULE-TIME **portlist** PORTLIST-ID **poe-action** { **on-port** | **off-port** | **off/on-port** }
- **no peth schedule** SCHEDULE-ID

Parameters

Parameter	Description
SCHEDULE-ID	Specifies the PoE schedule ID.
SCHEDULE-NAME	Specifies the name of the PoE schedule.
SCHEDULE-DATE	Specifies the date of the PoE schedule.
SCHEDULE-TIME	Specifies the time of the PoE schedule.
PORTLIST-ID	Specifies the port list ID which is controlled by the PoE schedule.
on-port	Turns ON the PoE power supply by the PoE schedule.
off-port	Turns OFF the PoE power supply by the PoE schedule.
off/on-port	Turns OFF/ON the PoE power supply by the PoE schedule.

Default

N/A

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guidelines

This command is used to configure the PoE schedule which is performed monthly.

Example

This example shows how to create PoE schedule ID: 3, schedule name: poe-name3, and to turn ON the PoE power supply at 20:21 on the 30th every month.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#peth schedule 3 name poe-name3 monthly date 30 time 20:21
portlist 1 poe-action on-port
GA-MLxxTPoE+(config)#
```

3.8.4 peth schedule weekly

This command is used to configure the PoE schedule which is performed weekly. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth schedule** SCHEDULE-ID **name** SCHEDULE-NAME **weekly** WEEKLY-DAY **time** SCHEDULE-TIME **portlist** PORTLIST-ID **poe-action** { **on-port** | **off-port** | **off/on-port** }
- **no peth schedule** SCHEDULE-ID

Parameters

Parameter	Description
SCHEDULE-ID	Specifies the PoE schedule ID.
SCHEDULE-NAME	Specifies the name of the PoE schedule.
WEEKLY-DAY	Specifies the day of week of the PoE schedule. (Sun,Mon,Tue,Wed,Thu,Fri,Sat)
SCHEDULE-TIME	Specifies the time of the PoE schedule.
PORTLIST-ID	Specifies the port list ID which is controlled by the PoE schedule.
on-port	Turns ON the PoE power supply by the PoE schedule.
off-port	Turns OFF the PoE power supply by the PoE schedule.
off/on-port	Turns OFF/ON the PoE power supply by the PoE schedule.

Default

N/A

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guidelines

This command is used to configure the PoE schedule which is performed weekly.

Example

This example shows how to create PoE schedule ID: 4, schedule name: poe-name4, and to turn OFF the PoE power supply at 10:30 every Sunday.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#peth schedule 4 name poe-name4 weekly sun time 10:30 portlist 1 poe-action off-port
GA-MLxxTPoE+(config)#
```

3.8.5 peth schedule daily

This command is used to configure the PoE schedule which is performed daily. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth schedule** SCHEDULE-ID **name** SCHEDULE-NAME **daily time** SCHEDULE-TIME **portlist** PORTLIST-ID **poe-action { on-port | off-port | off/on-port }**
- **no peth schedule** SCHEDULE-ID

Parameters

Parameter	Description
SCHEDULE-ID	Specifies the PoE schedule ID.
SCHEDULE-NAME	Specifies the name of the PoE schedule.
SCHEDULE-TIME	Specifies the time of the PoE schedule.
PORTLIST-ID	Specifies the port list ID which is controlled by the PoE schedule.
on-port	Turns ON the PoE power supply by the PoE schedule.
off-port	Turns OFF the PoE power supply by the PoE schedule.
off/on-port	Turns OFF/ON the PoE power supply by the PoE schedule.

Default

N/A

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guidelines

This command is used to configure the PoE schedule which is performed daily.

Example

This example shows how to create PoE schedule ID: 5, schedule name: poe-name5, and to turn OFF the PoE power supply at 2:23 every day.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#peth schedule 5 name poe-name5 daily time 2:23 portlist 1 poe-action off-port
GA-MLxxTPoE+(config)#
```

3.8.6 peth schedule datelist year

This command is used to configure the schedule date list of the PoE schedule. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth schedule datelist** DATELIST-ID **year** DATELIST-YEAR **name** DATELIST-NAME **days** DATELIST-DAYS
- **no peth schedule datelist** DATELIST-ID

Parameters

Parameter	Description
DATELIST-ID	Specifies the ID of the schedule date list.
DATELIST-YEAR	Specifies the year of the schedule date list.
DATELIST-NAME	Specifies the name of the schedule date list.
DATELIST-DAYS	Specifies the schedule date of the schedule date list.

Default

N/A

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guidelines

This command is used to configure the schedule date list of the PoE schedule.

Example

This example shows how to create a schedule list which is used for the schedule date list ID: 1, schedule date list name: test 2, execution year: 2019, and to configure a schedule date on May 21.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#peth schedule datelist 1 year 2019 name test2 days 5/21
GA-MLxxTPoE+(config)#
```

3.8.7 peth schedule datelist add

This command is used to add a schedule date to the schedule date list of the PoE schedule.

Syntax

- **peth schedule datelist** DATELIST-ID **add** DATELIST-DAYS

Parameters

Parameter	Description
DATELIST-ID	Specifies the ID of the schedule date list.
DATELIST-DAYS	Specifies the schedule date of the schedule date list.

Default

N/A

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guidelines

This command is used to add a schedule date to the schedule date list of the PoE schedule.

Example

This example shows how to add a schedule date October 10 to the schedule date list ID: 1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#peth schedule datelist 1 add 10/10
GA-MLxxTPoE+(config)#
```

3.8.8 peth schedule datelist delete

This command is used to delete a schedule date from the schedule date list of the PoE schedule.

Syntax

- **peth schedule datelist** DATELIST-ID **delete** DATELIST-DAYS

Parameters

Parameter	Description
DATELIST-ID	Specifies the ID of the schedule date list.
DATELIST-DAYS	Specifies the schedule date of the schedule date list.

Default

N/A

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guidelines

This command is used to delete a schedule date from the schedule date list of the PoE schedule.

Example

This example shows how to delete a schedule date October 10 from the schedule date list ID: 1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#peth schedule datelist 1 delete 10/10
GA-MLxxTPoE+(config)#
```

3.8.9 peth schedule datelist

This command is used to configure the PoE schedule which is performed on a schedule date. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth schedule** SCHEDULE-ID **name** SCHEDULE-NAME **datelist** DATELIST-ID **time** SCHEDULE-TIME **portlist** PORTLIST-ID **poe-action** { **on-port** | **off-port** | **off/on-port** }
- **no peth schedule** SCHEDULE-ID

Parameters

Parameter	Description
SCHEDULE-ID	Specifies the PoE schedule ID.
SCHEDULE-NAME	Specifies the name of the PoE schedule.
DATELIST-ID	Specifies the schedule date list ID of the PoE schedule.
SCHEDULE-TIME	Specifies the time of the PoE schedule.
PORTLIST-ID	Specifies the port list ID which is controlled by the PoE schedule.
on-port	Turns ON the PoE power supply by the PoE schedule.
off-port	Turns OFF the PoE power supply by the PoE schedule.
off/on-port	Turns OFF/ON the PoE power supply by the PoE schedule.

Default

N/A

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guidelines

This command is used to configure the PoE schedule which is performed on a schedule date.

Example

This example shows how to create PoE schedule ID: 6, schedule name: poe-name6, and to turn ON the PoE power supply at 10:30 on the schedule date list 1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#peth schedule 6 name poe-name6 datelist 1 time 10:30 portlist 1
poe-action on-port
GA-MLxxTPoE+(config)#
```

3.8.10 peth schedule portlist

This command is used to configure a port list of the PoE schedule. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth schedule portlist** PORTLIST-ID **member** PORTLIST
- **no peth schedule portlist** PORTLIST-ID

Parameters

Parameter	Description
PORTLIST-ID	Specifies the port list ID of the PoE schedule.
PORTLIST	Specify a port member which belongs to the port list.

Default

N/A

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guidelines

This command is used to configure a port list of the PoE schedule.

Example

This example shows how to configure Gi1/0/1 and Gi1/0/2 to port list ID 1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#peth schedule portlist 1 member gi1/0/1-2
GA-MLxxTPoE+(config)#
```

3.8.11 show peth schedule

This command is used to display the configuration of the PoE schedule.

Syntax

- show peth schedule

Parameters

N/A

Default

N/A

Command Mode

Privileged Mode

Command Default Level

Level:1

Usage Guidelines

This command is used to display the setting of the PoE schedule.

Example

This example shows how to display the configuration of the PoE schedule.

```
GA-MLxxTPoE+#show peth schedule
 PoE Schedule Global Status   : Enable
 Operation Status : Enable
 Sorting Method               : By Index
 PoE Schedule:                          Total Entries : 1
 Index Name              Class.  Port List Action Status   Next Execution Time
 ----- ----------------- ------- --------- ------ -------- -------------------
     6 poe-name6         DateList        1 ON     Enabled  2019/05/14 10:30

GA-MLxxTPoE+#
```

3.8.12 show peth schedule portlist

This command is used to display the port list setting of the PoE schedule.

Syntax

- **show peth schedule portlist**

Parameters

N/A

Default

N/A

Command Mode

Privileged Mode

Command Default Level

Level:1

Usage Guidelines

This command is used to display the port list setting of the PoE schedule.

Example

This example shows how to display the port list setting of the PoE schedule.

```
GA-MLxxTPoE+#show peth schedule portlist
 Port List :                          Total Entries : 1
 Index      Port List
 ------     ------------------------------------------------------------
      1     Gi1/0/1-1/0/2

GA-MLxxTPoE+#
```

3.8.13 show peth schedule datelist

This command is used to display the configuration of the schedule date list.

Syntax

- **show peth schedule datelist** {DATELIST-ID | **configuration**}

Parameters

Parameter	Description
DATELIST-ID	Displays the schedule date list of the PoE schedule.
configuration	Displays the execution setting of the schedule date list of the PoE schedule.

Default

N/A

Command Mode

Privileged Mode

Command Default Level

Level:1

Usage Guidelines

This command is used to display the setting of the schedule date list.

Example

This example shows how to display the configuration of the schedule date list.

```
GA-MLxxTPoE+#show peth schedule datelist configuration
Total Entries : 1
 Index   Date List    Year    Time    Act.   Status
 -----   ---------    ----    -----   -----  ------
     6           1    2020    10:30   ON     Enabled

GA-MLxxTPoE+#
```

This example shows how to display the setting of the schedule date list.

```
GA-MLxxTPoE+#show peth schedule datelist 1
 Date List Index : 1            Name : datelist1
 Year : 2020
 Date:
 Month    Day
 ------   ------------------------------------------------------------------
      1
      2
      3
      4
      5   14
      6
      7
      8
      9
     10
     11
     12

GA-MLxxTPoE+#
```

3.8.14 show peth schedule configuration-by-port

This command is used to display the PoE schedule setting of the specified port.

Syntax

- **show peth schedule configuration-by-port** INTERFACE-ID

Parameters

Parameter	Description
INTERFACE-ID	Displays the schedule date list of the PoE schedule.

Default

N/A

Command Mode

Privileged Mode

Command Default Level

Level:1

Usage Guidelines

This command is used to display the PoE schedule setting of the specified port.

Example

This example shows how to display the configuration of the PoE schedule of port 1.

```
GA-MLxxTPoE+#show peth schedule configuration-by-port 1
 Selected Port Number : 1

 PoE Schedule:                                      Total Entries : 1
 Index  Class.    Date                                  Time    Action  Status
 -----  -------   ------------------------------------ -----   ------  --------
     6  Datelist  Datelist 1                            10:30   ON      Enabled

GA-MLxxTPoE+#
```

3.8.15 show peth schedule information

This command is used to display the information of each PoE schedule ID.

Syntax

- **show peth schedule information** SCHEDULE-ID

Parameters

N/A

Default

N/A

Command Mode

Privileged Mode

Command Default Level

Level:1

Usage Guidelines

This command is used to display the information of each PoE schedule ID.

Example

This example shows how to display the information of each PoE schedule ID.

```
GA-MLxxTPoE+#show peth schedule information 6

 Detailed Schedule Information :
 ------------------------------------------------
 Schedule Index              : 6
 Schedule Name               : poe-name6
 Schedule Classifier         : Datelist
 Year                        : 2020
 Date                        : -
 Date List Index             : 1
 Time                        : 10:30
 Port List Index             : 1
 PoE Action                  : ON

GA-MLxxTPoE+#
```

3.9 PoE Auto Reboot

3.9.1 peth auto-reboot enable

This command is used to perform the global configuration of the PoE auto reboot function. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth auto-reboot enable**
- **no peth auto-reboot enable**

Parameters

N/A

Default

Disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guideline

The global configuration of PoE auto reboot function is performed.

Example

This example shows how to enable the global configuration of the PoE auto reboot function.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#peth auto-reboot enable
GA-MLxxTPoE+(config)#
```

3.9.2 peth auto-reboot ping address

This command is used to set the monitoring method of PoE auto reboot to Ping and to configure the IP address of the terminal. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth auto-reboot ping address** PING-ADDRESS
- **no peth auto-reboot ping address**

Parameters

Parameter	Description
PING-ADDRESS	Specifies the IP address of PoE terminal.

Default

N/A

Command Mode

Interface Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to configure the Ping monitoring of PoE auto reboot.

Example

This example shows how to configure the monitoring of PoE terminal 192.168.1.1 by sending Ping.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#peth auto-reboot ping address 192.168.1.1
GA-MLxxTPoE+(config-if)#
```

3.9.3 peth auto-reboot ping interval

This command is used to configure the Ping monitoring interval of PoE auto reboot. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth auto-reboot ping interval** PING-INTERVAL
- **no peth auto-reboot ping interval**

Parameters

Parameter	Description
PING-INTERVAL	Specifies the Ping monitoring interval. The range is from 1 to 86400 seconds.

Default

The default is 60 seconds.

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to set the Ping monitoring interval of PoE auto reboot.

Example

This example shows how to configure the Ping monitoring interval of PoE auto reboot to 90 seconds.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#peth auto-reboot ping interval 90
GA-MLxxTPoE+(config)#
```

3.9.4 peth auto-reboot ping timeout

This command is used to configure the timeout period of Ping monitoring of PoE auto reboot. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth auto-reboot ping timeout** PING-TIMEOUT
- **no peth auto-reboot ping timeout**

Parameters

Parameter	Description
PING-TIMEOUT	Specifies the timeout period of Ping monitoring. The range is from 1 to 30 seconds.

Default

The default is 5 seconds.

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to configure the timeout period of Ping monitoring of PoE auto reboot.

Example

This example shows how to configure the timeout period of Ping monitoring of PoE auto reboot to 3 seconds.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#peth auto-reboot ping timeout 3
GA-MLxxTPoE+(config)#
```

3.9.5 peth auto-reboot ping retry

This command is used to configure the retry frequency of Ping monitoring of PoE auto reboot. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth auto-reboot ping retry** ERROR-RETRY
- **no peth auto-reboot ping retry**

Parameters

Parameter	Description
ERROR-RETRY	Specifies the retry frequency of Ping monitoring. The range is from 1 to 10.

Default

Default is three times.

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to configure the retry frequency of Ping monitoring of PoE auto reboot.
If there is no response to Ping for a specified number of times, it is judged as abnormal.

Example

This example shows how to configure the retry frequency of Ping monitoring of PoE auto reboot to five times.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#peth auto-reboot ping retry 5
GA-MLxxTPoE+(config)#
```

3.9.6 peth auto-reboot lldp

This command is used to configure the monitoring method of PoE auto reboot to LLDP. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth auto-reboot lldp**
- **no peth auto-reboot lldp**

Parameters

N/A

Default

No default is configured.

Command Mode

Interface Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to set the monitoring method of PoE auto reboot to LLDP.

Example

This example shows how to configure the monitoring method of PoE auto reboot to LLDP.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#peth auto-reboot lldp
GA-MLxxTPoE+(config-if)#
```

3.9.7 peth auto-reboot lldp timeout

This command is used to configure the timeout period of LLDP monitoring of PoE auto reboot. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth auto-reboot lldp** LLDP-TIMEOUT
- **no peth auto-reboot lldp**

Parameters

Parameter	Description
LLDP-TIMEOUT	Specifies the timeout period of LLDP monitoring. The range is from 1 to 180 seconds.

Default

The default is 65 seconds.

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to configure the timeout period of LLDP monitoring.

Example

This example shows how to configure the timeout period of LLDP monitoring to 70 seconds.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#peth auto-reboot lldp timeout 70
GA-MLxxTPoE+(config)#
```

3.9.8 peth auto-reboot lldp retry

This command is used to configure the retry frequency of LLDP monitoring of PoE auto reboot. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth auto-reboot lldp retry** ERROR-RETRY
- **no peth auto-reboot lldp retry**

Parameters

Parameter	Description
ERROR-RETRY	Specifies the retry frequency of LLDP monitoring. The range is from 1 to 10.

Default

The default is three times.

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to configure the retry frequency of LLDP monitoring of PoE auto reboot.

Example

This example shows how to configure the retry frequency of LLDP monitoring of PoE auto reboot to two times.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#peth auto-reboot lldp retry 2
GA-MLxxTPoE+(config)#
```

3.9.9 peth auto-reboot traffic

This command is used to configure the monitoring method of PoE auto reboot to the traffic (communication traffic) monitoring. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth auto-reboot traffic** {**over** | **below**} {TRAFFIC-THRESHOLD | **percentage** {percentage} }
- **no peth auto-reboot traffic**

Parameters

Parameter	Description
over	Judges the PoE terminal to be abnormal when the communication traffic exceeded the threshold.
below	Judges the PoE terminal to be abnormal when the communication traffic fell below the threshold.
TRAFFIC-THRESHOLD	Specifies the threshold of communication traffic in bps. The range is from 0 to 1000000000 (bps).
percentage	Specifies the threshold of communication traffic in %. The range is from 0 to 100 (%).

Default

N/A

Command Mode

Interface Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to configure the monitoring method of PoE auto reboot to the traffic monitoring.

Example

This example shows how to configure to judge as abnormal when the traffic of port 1 falls below 1 Mbps (1000000 bps).

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config)#peth auto-reboot traffic below 1000000
GA-MLxxTPoE+(config)#
```

3.9.10 peth auto-reboot traffic average

This command is used to configure the average time of the traffic measurement of PoE auto reboot. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth auto-reboot traffic average** AVERAGE-TIME
- **no peth auto-reboot traffic average**

Parameters

Parameter	Description
AVERAGE-TIME	Specifies the average time of traffic measurement. The range is from 1 to 60 seconds.

Default

The default is 5 seconds.

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to configure the average time of the traffic measurement of PoE auto reboot.

Example

This example shows how to configure the average time of the traffic measurement of PoE auto reboot to 10 seconds.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#peth auto-reboot traffic average 10
GA-MLxxTPoE+(config)#
```

3.9.11 peth auto-reboot traffic interval

This command is used to configure the traffic monitoring interval of PoE auto reboot. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth auto-reboot traffic interval** TRAFFIC-INTERVAL
- **no peth auto-reboot traffic interval**

Parameters

Parameter	Description
TRAFFIC-INTERVAL	Specifies the traffic monitoring interval. The range is from 1 to 60 seconds.

Default

The default is 5 seconds.

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to configure the traffic monitoring interval of PoE auto reboot.

Example

This example shows how to configure the traffic monitoring interval of PoE auto reboot to 10 seconds.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#peth auto-reboot traffic interval 10
GA-MLxxTPoE+(config)#
```

3.9.12 peth auto-reboot traffic retry

This command is used to configure the retry frequency of the traffic monitoring of PoE auto reboot. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth auto-reboot traffic retry** ERROR-RETRY
- **no peth auto-reboot traffic retry**

Parameters

Parameter	Description
ERROR-RETRY	Specifies the retry frequency of traffic monitoring. The range is from 1 to 10.

Default

Default is three times.

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to configure the retry frequency of the traffic monitoring of PoE auto reboot.

Example

This example shows how to configure the retry frequency of the traffic monitoring of PoE auto reboot to two times.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#peth auto-reboot traffic retry 2
GA-MLxxTPoE+(config)#
```

3.9.13 peth auto-reboot notify

This command is used to configure the PoE power supply OFF/ON control and the notification method when the PoE auto reboot judged as abnormal. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth auto-reboot notify {poe | smtp | trap}**
- **no peth auto-reboot notify {poe | smtp | trap}**

Parameters

Parameter	Description
poe	Enables the PoE power supply OFF/ON when the PoE auto reboot detected abnormality.
smtp	Enables the mail notification when the PoE auto reboot detected abnormality.
trap	Enables the SNMP trap when the PoE auto reboot detected abnormality.

Default

PoE power supply OFF/ON : Enabled
Mail notification : Disabled
SNMP trap notification : Disabled

Command Mode

Interface Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to configure the PoE power supply OFF/ON control and the notification method when the PoE auto reboot judged as abnormal. Until the actual power supply OFF or ON is processed, it may take approximately 15 seconds.

Example

This example shows how to enable the SNMP trap notification when the PoE auto reboot judged as abnormal.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#peth auto-reboot notify trap
GA-MLxxTPoE+(config)#
```

3.9.14 peth auto-reboot off-interval

This command is used to configure the interval between the OFF control and ON control of the PoE power supply of PoE auto reboot. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth auto-reboot off-interval** OFF-INTERVAL
- **no peth auto-reboot off-interval**

Parameters

Parameter	Description
OFF-INTERVAL	Specifies the interval between the OFF control and the ON control of the PoE power supply of PoE auto reboot. The range is from 1 to 30 seconds.

Default

The default is 3 seconds.

Command Mode

Interface Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to configure the interval between the OFF control and ON control of the PoE power supply of PoE auto reboot. The interval should be changed when the PoE terminal does not reboot successfully.

Example

This example shows how to configure the interval between the OFF control and the ON control of the PoE power supply of PoE auto reboot to 5 seconds.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#peth auto-reboot off-interval 5
GA-MLxxTPoE+(config)#
```

3.9.15 peth auto-reboot repeat

This command is used to enable the repetition control of PoE power supply OFF/ ON until the abnormality of PoE terminal is dissolved. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth auto-reboot repeat**
- **no peth auto-reboot repeat**

Parameters

N/A

Default

The default is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to enable the repetition control of PoE power supply OFF/ ON until the abnormality of PoE terminal is dissolved.

Example

This example shows how to enable the repetition control of PoE power supply OFF/ON.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#peth auto-reboot repeat
GA-MLxxTPoE+(config)#
```

3.9.16 peth auto-reboot repeat-interval

This command is used to configure the interval of repetition control of PoE power supply OFF/ON until the abnormality of PoE terminal is dissolved. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth auto-reboot repeat-interval** REPEAT-INTERVAL
- **no peth auto-reboot repeat-interval**

Parameters

Parameter	Description
REPEAT-INTERVAL	Specifies the repetition interval of PoE power supply OFF/ON. The range is from 1 to 86400 seconds.

Default

The default is 600 seconds.

Command Mode

Interface Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to configure the repetition interval of PoE power supply OFF/ON.

Example

This example shows how to configure the repetition interval of PoE power supply OFF/ON to 120 seconds.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#peth auto-reboot repeat-interval 120
GA-MLxxTPoE+(config)#
```

3.9.17 peth auto-reboot judge-condition

This command is used to configure the abnormality judgment condition of PoE auto reboot. Use the **no** form of the command to revert to the default setting.

Syntax

- **peth auto-reboot judge-condition {and | or }**
- **no peth auto-reboot judge-condition**

Parameters

Parameter	Description
and	Judges as abnormal when all monitoring methods (Ping, LLDP, and traffic) detected abnormality.
or	Judges as abnormal when any of the monitoring methods (Ping, LLDP, and traffic) detected abnormality.

Default

The default is **or**.

Command Mode

Interface Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to configure the abnormality judgment condition of PoE auto reboot.

Example

This example shows how to configure the abnormality judgment condition of PoE auto reboot to judge as abnormal when all monitoring methods detected abnormality.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#peth auto-reboot judge-condition or
GA-MLxxTPoE+(config)#
```

3.9.18 show peth auto-reboot

This command is used to display the configuration of PoE auto reboot.

Syntax

- show peth auto-reboot

Parameters

N/A

Default

N/A

Command Mode

Privileged Mode

Command Default Level

Level:1

Usage Guideline

This command is used to display the configuration of PoE auto reboot.

Example

This example shows how to display the configuration of PoE auto reboot.

```
GA-MLxxTPoE+#show peth auto-reboot

PoE Auto Reboot Global Status : Enabled
PoE Auto Reboot SMTP Mail Subject :
PoE Auto Reboot SMTP Mail Content :

            Judge     Send      Snmp      PoE     PoE OFF/ON  PoE OFF/ON    Repeat
   Port   Condition  Email     Trap     OFF/ON    Interval     Repeat     Interval
 -------- --------- ------- -------- -------- ---------- ---------- ----------
 Gi1/0/1     AND    Enable   Enable   Disable    10        Enable        600
 Gi1/0/2     OR     Disable  Disable  Enable      3        Disable       600
 Gi1/0/3     OR     Disable  Disable  Enable      3        Disable       600
 Gi1/0/4     OR     Disable  Disable  Enable      3        Disable       600

GA-MLxxTPoE+#
```

3.9.19 show peth auto-reboot ping

This command is used to display the Ping monitoring setting of PoE auto reboot.

Syntax

- show peth auto-reboot ping

Parameters

N/A

Default

N/A

Command Mode

Privileged Mode

Command Default Level

Level:1

Usage Guideline

This command is used to display the Ping monitoring setting of PoE auto reboot.

Example

This example shows how to display the Ping monitoring setting of PoE auto reboot.

```
GA-MLxxTPoE+#show peth auto-reboot ping

 Ping Interval    : 60
 Ping Time out    : 5
 Ping Error Retry : 3

    Port       Ping IP address
 ----------  ---------------------
  Gi1/0/1      192.168.1.1
  Gi1/0/2
  Gi1/0/3
  Gi1/0/4

GA-MLxxTPoE+#in
```

3.9.20 show peth auto-reboot lldp

This command is used to display the LLDP monitoring setting of PoE auto reboot.

Syntax

- show peth auto-reboot lldp

Parameters

N/A

Default

N/A

Command Mode

Privileged Mode

Command Default Level

Level:1

Usage Guideline

This command is used to display the LLDP monitoring setting of PoE auto reboot.

Example

This example shows how to display the LLDP monitoring setting of PoE auto reboot.

```
GA-MLxxTPoE+#show peth auto-reboot lldp

 LLDP Time out    : 65
 LLDP Error Retry : 3

    Port         Status
 ----------  --------------
  Gi1/0/1      Enabled
  Gi1/0/2      Disabled
  Gi1/0/3      Disabled
  Gi1/0/4      Disabled

GA-MLxxTPoE+#
```

3.9.21 show peth auto-reboot traffic

This command is used to display the traffic monitoring setting of PoE auto reboot.

Syntax

- show peth auto-reboot traffic

Parameters

N/A

Default

N/A

Command Mode

Privileged Mode

Command Default Level

Level:1

Usage Guideline

This command is used to display the traffic monitoring setting of PoE auto reboot.

Example

This example shows how to display the traffic monitoring setting of PoE auto reboot.

```
GA-MLxxTPoE+#show peth auto-reboot traffic

 Traffic Average     : 5
 Traffic Interval    : 5
 Traffic Error Retry : 3

    Port      Judge Condition    Traffic Threshold
 ----------  -----------------  -------------------
  Gi1/0/1          Below                1000000
  Gi1/0/2          Over                20000000
  Gi1/0/3          None
  Gi1/0/4          None

GA-MLxxTPoE+#
```

4 L2 Switching

4.1 FDB (Filter Database) Commands

4.1.1 clear mac-address-table

This command is used to delete a specific dynamic MAC address, all dynamic MAC addresses on a particular interface, all dynamic MAC addresses on a particular VLAN, or all dynamic MAC addresses from the MAC address table.

Syntax

- **clear mac-address-table dynamic {all | address** *MAC-ADDR* **| interface** *INTERFACE-ID* **| vlan** *VLAN-ID*}

Parameters

Parameters	Description
all	Specifies to clear all dynamic MAC addresses.
address *MAC-ADDR*	Specifies to delete the specified dynamic MAC address.
interface *INTERFACE-ID*	Specifies the interface that the MAC address will be deleted from. The specified interface can be a physical port or a port-channel.
vlan *VLAN-ID*	Specifies the VLAN ID. The valid values are from 1 to 4094.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guidelines

Use this command to only clear dynamic MAC address entries. Only the dynamic unicast address entry will be cleared.

Example

This example shows how to remove the MAC address 00:50:40:70:00:07 from the dynamic MAC address table.

```
GA-MLxxTPoE+# clear mac-address-table dynamic address 00:50:40:70:00:07
GA-MLxxTPoE+#
```

4.1.2 mac-address-table aging-time

This command is used to configure the MAC address table aging time. Use the **no** form of this command to revert to the default setting.

Syntax

- **mac-address-table aging-time** *SECONDS*
- **no mac-address-table aging-time**

Parameters

Parameters	Description
SECONDS	Specifies the aging time in seconds. The valid range is 0 or 10 to 1000000 seconds. Setting the aging time to 0 will disable the MAC address table aging out function.

Default

By default, this value is 300 seconds.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Setting the aging time to 0 will disable the MAC address table aging out function.

Example

This example shows how to set the aging time value to 200 seconds.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# mac-address-table aging-time 200
GA-MLxxTPoE+(config)#
```

4.1.3 mac-address-table aging destination-hit

This command is used to enable the destination MAC address triggered update function. Use the **no** form of this command to disable the destination MAC address triggered updated function.

Syntax

- **mac-address-table aging destination-hit**
- **no mac-address-table aging destination-hit**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

The source MAC address triggered update function is always enabled. The hit bit of MAC address entries corresponding to the port that receives the packet will be updated based on the source MAC address and the VLAN of the packet. When the user enables the destination MAC address triggered update function by using the **mac-address-table aging destination-hit** command, the hit bit of MAC address entries corresponding to the port that transmit the packet will be updated based on the destination MAC address and the VLAN of the packet.

The destination MAC address triggered update function increases the MAC address entries hit bit update frequency and reduce traffic flooding by the MAC address entries aging time-out.

Example

This example shows how to enable the destination MAC address triggered update function.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# mac-address-table aging destination-hit
GA-MLxxTPoE+(config)#
```

4.1.4 mac-address-table learning

This command is used to enable MAC address learning on the physical port or VLAN. Use the **no** form of this command to disable learning.

Syntax

- **mac-address-table learning interface** {**vlan** *VLAN-ID* [**,** | **-**] | *INTERFACE-ID* [**,** | **-**]}
- **no mac-address-table learning interface** {**vlan** *VLAN-ID* [**,** | **-**] | *INTERFACE-ID* [**,** | **-**]}

Parameters

Parameters	Description
vlan *VLAN-ID*	Specifies the VLAN ID to be configured.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.
INTERFACE-ID	Specifies the physical port interface to be configured.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use this commands to enable or disable MAC address learning on a physical port or VLAN.
The behavior of MAC addresses learning on VLAN interfaces:
By default, MAC address learning is always enabled on all VLANs on the Switch when VLAN is created. MAC address learning will be recovered to the default value when a VLAN is deleted.
MAC address learning only can be configured on the existed VLAN.
Disabling MAC address learning on a VLAN will cause all ports belong to this VLAN stop the MAC address learning.
Disabling MAC address learning on the voice or surveillance VLAN, the function will work abnormally based on MAC address learning.
Disabling MAC address learning on a VLAN will cause asymmetric VLAN work abnormally on the related VLAN.
Disabling MAC address learning on a private VLAN will cause related private VLAN work abnormally.
RSPAN VLAN has the higher precedence, and MAC address learning is always disabled on the RSPAN VLAN. If RSPAN VLAN is deleted, the configured MAC address learning state takes effect.
The MAC address learning for the secure modules such as Port Security, 802.1x, MAC-based Access Control, Web-based Access Control and IMPB has the higher precedence. If MAC address learning on a VLAN that includes a secure port is disabled, MAC address learning is not disabled on the VLAN. If all the secure ports on the VLAN are disabled, the configured MAC address learning state takes effect.

NOTE Secure modules are port security, 802.1X, MAC-based access control, WAC, and IP-MAC-Port binding.

Example

This example shows how to enable the MAC address learning option.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# mac-address-table learning interface gi1/0/5
GA-MLxxTPoE+(config)#
```

4.1.5 mac-address-table notification change

This command is used to enable or configure the MAC address notification function. Use the **no** form of this command to disable the function or set the optional configuration to default.

Syntax

- **mac-address-table notification change** [**interval** *SECONDS* | **history-size** *VALUE*]
- **no mac-address-table notification change** [**interval** | **history-size**]

Parameters

Parameters	Description
interval *SECONDS*	(Optional) Specifies the interval of sending the MAC address trap message. The range is from 1 to 2147483647 and the default value is 1 second.
history-size *VALUE*	(Optional) Specifies the maximum number of the entries in the MAC history notification table. The range is 0 to 500 and the default value is 1 entry.

Default

MAC address notification is disabled.
The default trap interval is 1 second.
The default number of entries in the history table is 1.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

When the Switch learns or removes a MAC address, a notification can be sent to the notification history table and then sent to the SNMP server if the **snmp-server enable traps mac-notification change** command is enabled. The MAC notification history table stores the MAC address learned or deleted on each interface for which the trap is enabled. Events are not generated for multicast addresses.

Example

This example shows how to enable MAC address change notification and set the interval to 10 seconds and set the history size value to 500 entries.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# mac-address-table notification change
GA-MLxxTPoE+(config)# mac-address-table notification change interval 10
GA-MLxxTPoE+(config)# mac-address-table notification change history-size 500
GA-MLxxTPoE+(config)#
```

4.1.6 mac-address-table static

This command is used to add a static address to the MAC address table. Use the **no** form of the command to remove a static MAC address entry from the table.

Syntax

- **mac-address-table static** *MAC-ADDR* **vlan** *VLAN-ID* {**interface** *INTERFACE-ID* [**,** | **-**] | **drop**}
- **no mac-address-table static** {**all** | *MAC-ADDR* **vlan** *VLAN-ID* [**interface** *INTERFACE-ID*] [**,** | **-**]}

Parameters

Parameters	Description
MAC-ADDR	Specifies the MAC address of the entry. The address can be a unicast or a multicast entry. Packets with a destination address that match this MAC address received by the specified VLAN are forwarded to the specified interface.
vlan *VLAN-ID*	Specifies the VLAN of the entry. The range is from 1 to 4094.
interface *INTERFACE-ID*	Specifies the forwarding ports.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
drop	Specifies to drop the frames that are sent by or sent to the specified MAC address on the specified VLAN.
all	Specifies to remove all static MAC address entries.

Default

No static addresses are configured.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

For a unicast MAC address entry, only one interface can be specified. For a multicast MAC address entry, multiple interfaces can be specified. To delete a unicast MAC address entry, there is no need to specify the interface ID. To delete a multicast MAC address entry, if an interface ID is specified, only this interface will be removed. Otherwise, the entire multicast MAC entry will be removed. The **drop** parameter can only be specified for a unicast MAC address entry.

Example

This example shows how to add the static address C2:F3:22:0A:12:F4 to the MAC address table. It also specifies that when any packet received on VLAN 4 that has a destination MAC address of 00:50:40:0A:12:F4 will be forwarded to Gigabit Ethernet port 1/0/1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#mac-address-table static 00:50:40:0A:12:F4 vlan 4 interface gi1/0/1
GA-MLxxTPoE+(config)#
```

4.1.7 multicast filtering-mode

This command is used to configure the handling method for multicast packets for an interface. Use the **no** form of this command to revert to the default setting.

Syntax

- **multicast filtering-mode {forward-all | forward-unregistered | filter-unregistered}**
- **no multicast filtering-mode**

Parameters

Parameters	Description
forward-all	Specifies to flood all multicast packets based on the VLAN domain.

Parameters	Description
forward-unregistered	Specifies to forward registered multicast packets based on the forwarding table and flood all unregistered multicast packets based on the VLAN domain.
filter-unregistered	Specifies to forward registered packets based on the forwarding table and filter all unregistered multicast packets.

Default

By default, the forward-unregistered option is enabled.

Command Mode

VLAN Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

This filtering mode is only applied to multicast packets that are destined for addresses other than those reserved for multicast addresses.

Example

This example shows how to set the multicast filtering mode on VLAN 100 to filter unregistered.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 100
GA-MLxxTPoE+(config-vlan)# multicast filtering-mode filter-unregistered
GA-MLxxTPoE+(config-vlan)#
```

4.1.8 show mac-address-table

This command is used to display a specific MAC address entry or the MAC address entries for a specific interface or VLAN.

Syntax

- show mac-address-table [dynamic | static] [address *MAC-ADDR* | interface *INTERFACE-ID* | vlan *VLAN-ID*]

Parameters

Parameters	Description
dynamic	(Optional) Specifies to display dynamic MAC address table entries only.
static	(Optional) Specifies to display static MAC address table entries only.
address *MAC-ADDR*	(Optional) Specifies the 48-bit MAC address.
interface *INTERFACE-ID*	(Optional) Specifies to display information for a specific interface. Valid interfaces include physical ports and port-channels.
vlan *VLAN-ID*	(Optional) Specifies the VLAN ID. The valid values are from 1 to 4094.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guidelines

If the **interface** parameter is specified, the unicast entry that has the forwarding interface matches the specified interface will be displayed

Example

This example shows how to display all the MAC address table entries for the MAC address 00-23-7D-BC-08-44.

```
GA-MLxxTPoE+#show mac-address-table address 00-23-7D-BC-08-44

VLAN  MAC Address        Type        Ports
----  -----------------  ----------  -------------------------
1     00-23-7D-BC-08-44  Dynamic     Gi1/0/1

Total Entries: 1

GA-MLxxTPoE+#
```

This example shows how to display all the static MAC address table entries.

```
GA-MLxxTPoE+#show mac-address-table static

VLAN  MAC Address        Type        Ports
----  -----------------  ----------  -------------------------
1     00-50-40-xx-xx-xx  Static      CPU
4     C2-F3-22-0A-12-F4  Static      Gi1/0/1

Total Entries: 2

GA-MLxxTPoE+#
```

This example shows how to display all the MAC address table entries for VLAN 1.

```
GA-MLxxTPoE+#show mac-address-table vlan 1

VLAN  MAC Address        Type        Ports
----  -----------------  ----------  -------------------------
1     00-23-7D-BC-08-44  Dynamic     Gi1/0/1
1     00-23-7D-BC-2E-18  Dynamic     Gi1/0/1
1     00-50-40-xx-xx-xx  Static      CPU
1     00-FF-47-77-70-B8  Dynamic     Gi1/0/1
1     10-BF-48-D6-E2-E2  Dynamic     Gi1/0/1
1     5C-33-8E-43-B3-68  Dynamic     Gi1/0/1
1     D0-AE-EC-C4-E3-80  Dynamic     Gi1/0/1

Total Entries: 7

GA-MLxxTPoE+#
```

4.1.9 show mac-address-table aging-time

This command is used to display the aging time of the MAC address table.

Syntax

- **show mac-address-table aging-time**

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guidelines

This command is used to display the aging time of the MAC address table.

Example

This example shows how to display the aging time of the MAC address table.

```
GA-MLxxTPoE+# show mac-address-table aging-time

 Aging Time is 300 seconds.

GA-MLxxTPoE+#
```

4.1.10 show mac-address-table learning

This command is used to display the MAC-address learning state.

Syntax

- **show mac-address-table learning interface [vlan [***VLAN-ID* **[, | -]] | *INTERFACE-ID* [, | -]]**

Parameters

Parameters	Description
VLAN-ID	(Optional) Specifies the VLAN ID to be displayed. If not specified, all VLANs will be displayed.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.
INTERFACE-ID	(Optional) Specifies the interface to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guidelines

If no optional parameter is specified, all physical ports will be displayed.

Example

This example shows how to display the MAC address learning status on port 1-10.

```
GA-MLxxTPoE+#show mac-address-table learning interface gi 1/0/1-10

Port                        Status
--------------------------  --------
Gi1/0/1                     Enabled
Gi1/0/2                     Enabled
Gi1/0/3                     Enabled
Gi1/0/4                     Enabled
Gi1/0/5                     Enabled
Gi1/0/6                     Enabled
Gi1/0/7                     Enabled
Gi1/0/8                     Enabled
Gi1/0/9                     Enabled
Gi1/0/10                    Enabled

GA-MLxxTPoE+#
```

4.1.11 show mac-address-table notification change

This command is used to display the MAC address notification configuration or history content.

Syntax

- **show mac-address-table notification change [interface [*INTERFACE-ID*] | history]**

Parameters

Parameters	Description
interface *INTERFACE-ID*	(Optional) Specifies the interface to display.
history	(Optional) Specifies to display the MAC address notification change history.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guidelines

If no optional parameter is specified, the global configuration will be displayed. Use the **interface** parameter without an interface ID to display information related to all interfaces. If the interface ID is included, information related to the specified interface will be displayed.

Example

This example shows how to display the MAC address notification change configuration on all interfaces.

```
GA-MLxxTPoE+#show mac-address-table notification change interface

Interface                Added Trap       Removed Trap
-----------------------  --------------   --------------
Gi1/0/1                  Disabled         Disabled
Gi1/0/2                  Disabled         Disabled
Gi1/0/3                  Disabled         Disabled
Gi1/0/4                  Disabled         Disabled
Gi1/0/5                  Disabled         Disabled
Gi1/0/6                  Disabled         Disabled
Gi1/0/7                  Disabled         Disabled
Gi1/0/8                  Disabled         Disabled
Gi1/0/9                  Disabled         Disabled
Gi1/0/10                 Disabled         Disabled
Gi1/0/11                 Disabled         Disabled
Gi1/0/12                 Disabled         Disabled
Gi1/0/13                 Disabled         Disabled
Gi1/0/14                 Disabled         Disabled
Gi1/0/15                 Disabled         Disabled
Gi1/0/16                 Disabled         Disabled
Gi1/0/17                 Disabled         Disabled
Gi1/0/18                 Disabled         Disabled
Gi1/0/19                 Disabled         Disabled
Gi1/0/20                 Disabled         Disabled
Gi1/0/21                 Disabled         Disabled
--More--
```

This example shows how to display the MAC address notification global configuration.

```
GA-MLxxTPoE+#show mac-address-table notification change

MAC Notification Change Feature: Disabled
Interval between Notification Traps: 1 seconds
Maximum Number of Entries Configured in History Table: 1
Current History Table Length: 0
MAC Notification Trap State: Disabled

GA-MLxxTPoE+#
```

This example shows how to display the MAC address notification history.

```
GA-MLxxTPoE+#show mac-address-table notification change history

History Index: 1
Operation:ADD Vlan: 1 MAC Address: 00-f8-d0-12-34-56 gi1/0/1
History Index: 2
Operation:DEL Vlan: 1 MAC Address: 00-f8-d0-00-00-01 te1/0/26
History Index: 3
Operation:DEL Vlan: 1 MAC Address: 00-f8-d0-00-00-02 fo1/0/1

GA-MLxxTPoE+#
```

4.1.12 show multicast filtering-mode

This command is used to display the filtering mode for handling multicast packets that are received on an interface.

Syntax

- **show multicast filtering-mode [interface** *INTERFACE-ID*]

Parameters

Parameters	Description
interface *INTERFACE-ID*	(Optional) Specifies the VLAN to display.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guidelines

If no optional parameter is specified, all existing VLAN will be displayed.

Example

This example shows how to display the multicast filtering mode configuration for all VLANs.

```
GA-MLxxTPoE+# show multicast filtering-mode

Interface                       Layer 2 Multicast Filtering Mode
------------------------------- -------------------------------
default                         forward-unregistered

Total Entries: 1

GA-MLxxTPoE+#
```

4.1.13 snmp-server enable traps mac-notification change

This command is used to enable the sending of SNMP MAC notification traps. Use the **no** form of this command to disable the sending of SNMP MAC notification traps.

Syntax

- **snmp-server enable traps mac-notification change**
- **no snmp-server enable traps mac-notification change**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use this command to enable the sending of SNMP MAC notification traps.

Example

This example shows how to enable the sending of SNMP MAC notification traps.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server enable traps mac-notification change
GA-MLxxTPoE+(config)#
```

4.1.14 snmp trap mac-notification change

This command is used to enable the MAC address change notification on a specific interface. Use the **no** form of this command to revert to the default setting.

Syntax

- **snmp trap mac-notification change {added | removed}**
- **no snmp trap mac-notification change{added | removed}**

Parameters

Parameters	Description
added	Specifies to enable the MAC change notification when a MAC address is added on the interface.
removed	Specifies to enable the MAC change notification when a MAC address is removed from the interface.

Default

The traps for both address addition and address removal are disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Even when enabling the notification trap for a specific interface by using the **snmp trap mac-notification change** command, the notification is sent to the notification history table only when the **mac-address-table notification change** command was enabled.

Example

This example shows how to enable the MAC address added notification trap on Gigabit Ethernet port 1/0/2.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/2
GA-MLxxTPoE+(config-if)# snmp trap mac-notification change added
GA-MLxxTPoE+(config-if)#
```

4.2 Link Aggregation Control Protocol (LACP) Commands

Link aggregation is a technology to connect two switches with multiple ports and bundle them as one port. This provides path redundancy and enhanced bandwidth.
You can select how to distribute communications to bundled ports from several methods.

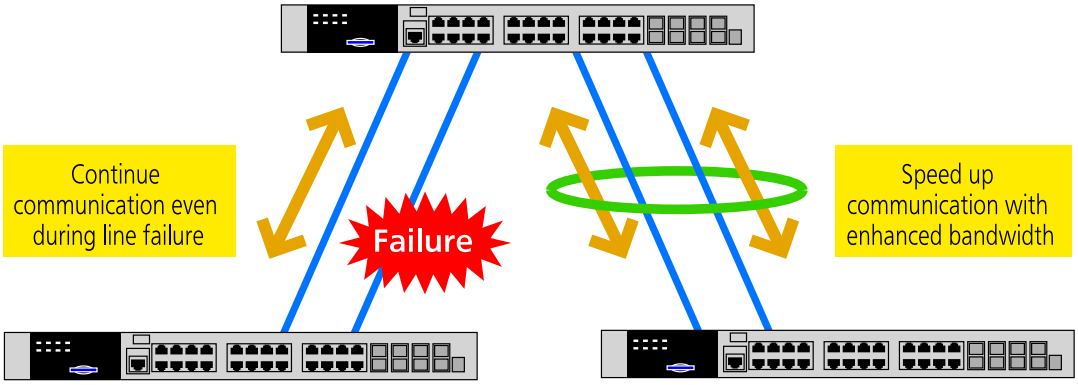


Figure 29-1 Link aggregation overview

4.2.1 channel-group

This command is used to assign an interface to a channel group. Use the **no** form of this command to remove an interface from a channel-group.

Syntax

- **channel-group** *CHANNEL-NO* **mode {on | active | passive}**
- **no channel-group**

Parameters

Parameters	Description
CHANNEL-NO	Specifies the channel group ID. The valid range is 1 to 48.
on	Specifies that the interface is a static member of the channel-group.

Parameters	Description
active	Specifies the interface to operate in LACP active mode.
passive	Specifies the interface to operate in LACP passive mode.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is available for physical port interface configuration. The system will automatically create the port-channel when a physical port first joins a channel group. An interface can only join one channel-group.
If the mode **on** is specified in the command, the channel group type is static. If the mode **active** or **passive** is specified in the command, the channel group type is LACP. A channel group can only consist of either static members or LACP members. Once the type of channel group has been determined, other types of interfaces cannot join the channel group.
If the security function is enabled on a port, then this port cannot be specified as a channel group member.
For instance, if you use the command, the VLAN configuration on the physical port interface becomes disabled. The configuration on the port channel interface becomes enabled.

Example

This example shows how to assign Ethernet interfaces 1/0/4 to 1/0/5 to a new LACP channel-group, with an ID of 3, and sets the LACP mode to active.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface range gi1/0/4-1/0/5
GA-MLxxTPoE+(config-if)# channel-group 3 mode active
GA-MLxxTPoE+(config-if)#
```

4.2.2 lacp port-priority

This command is used to configure the port priority. Use the **no** form of this command to revert to the default setting.

Syntax

- **lacp port-priority** *PRIORITY*
- **no lacp port-priority**

Parameters

Parameters	Description
PRIORITY	Specifies the port priority. The range is from 1 to 65535.

Default

The default port-priority is 32768.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The LACP port-priority determines which ports can join a port-channel and which ports are put in the standalone mode. The lower value has a higher priority. If two or more ports have the same priority, the port number determines the priority

Example

This example shows how to configure the port priority to 20000 on interfaces 1/0/4 to 1/0/5.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface range gi1/0/4-1/0/5
GA-MLxxTPoE+(config-if)# lacp port-priority 20000
GA-MLxxTPoE+(config-if)#
```

4.2.3 lacp timeout

This command is used to configure the LACP long or short timer. Use the **no** form of this command to revert to the default setting.

Syntax

- **lacp timeout {short | long}**
- **no lacp timeout**

Parameters

Parameters	Description
short	Specifies that there will be 3 seconds before invalidating received LACPDU information and there will be 1 second between LACP PDU periodic transmissions when the link partner uses Short Timeouts.
long	Specifies that there will be 90 seconds before invalidating received LACPDU information and there will be 30 seconds between LACP PDU periodic transmissions when the link partner uses Long Timeouts.

Default

By default, the LACP timeout mode is short.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is available for physical port interface configuration.

Example

This example shows how to configure the port LACP timeout to long mode on GigabitEthernet interface 1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# lacp timeout long
GA-MLxxTPoE+(config-if)#
```

4.2.4 lacp system-priority

This command is used to configure the system priority. Use the **no** form of this command to revert to the default setting.

Syntax

- **lacp system-priority** *PRIORITY*
- **no lacp system-priority**

Parameters

Parameters	Description
PRIORITY	Specifies the system priority. The range is from 1 to 65535.

Default

The default LACP system-priority is 32768.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

During LACP negotiation, the system priority and port priority of the local partner will be exchanged with the remote partner. The Switch will use port priority to determine whether a port is operating in a backup mode or in an active mode. The LACP system-priority determines the Switch that controls the port priority. Port priorities on the other switch are ignored.
The lower value has a higher priority. If two switches have the same system priority, the LACP system ID (MAC) determines the priority. The LACP system priority command applies to all LACP port-channels on the Switch.

Example

This example shows how to configure the LACP system priority to be 30000.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# lacp system-priority 30000
GA-MLxxTPoE+(config)#
```

4.2.5 port-channel load-balance

This command is used to configure the load-balancing algorithm that the Switch uses to distribute packets across ports in the same channel. Use the **no** form of this command to revert to the default setting.

Syntax

- **port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}**
- **no port-channel load-balance**

Parameters

Parameters	Description
dst-ip	Specifies that the Switch should examine the IP destination address.
dst-mac	Specifies that the Switch should examine the MAC destination address.
src-dst-ip	Specifies that the Switch should examine the IP source address and IP destination address.
src-dst-mac	Specifies that the Switch should examine the MAC source and MAC destination address.
src-ip	Specifies that the Switch should examine the IP source address.
src-mac	Specifies that the Switch should examine the MAC source address.

Default

The default load-balancing algorithm is **src-dst-mac**.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to specify the load balance algorithm. Only one algorithm can be specified.

Example

This example shows how to configure the load-balancing algorithm as **src-ip**.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# port-channel load-balance src-ip
GA-MLxxTPoE+(config)#
```

4.2.6 show channel-group

This command is used to display the channel group information.

Syntax

- **show channel-group [channel [***CHANNEL-NO***] {detail | neighbor} | load-balance | sys-id]**

Parameters

Parameters	Description
channel	(Optional) Specifies to display information for the specified port-channels.
CHANNEL-NO	(Optional) Specifies the channel group ID.
detail	(Optional) Specifies to display detailed channel group information.
neighbor	(Optional) Specifies to display neighbor information.
load-balance	(Optional) Specifies to display the load balance information.
sys-id	(Optional) Specifies to display the system identifier that is being used by LACP.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

If a port-channel number is not specified, all port-channels will be displayed. If the channel, **load-balance** and **sys-id** keywords are not specified with the **show channel-group** command, only summary channel-group information will be displayed.

Example

This example shows how to display the detailed information of all port-channels.

```
GA-MLxxTPoE+#show channel-group channel detail

Flag:
  S - Port is requesting Slow LACPDUs   F - Port is requesting fast LACPDU
  A - Port is in active mode            P - Port is in passive mode
LACP state:
  bndl:     Port is attached to an aggregator and bundled with other ports.
  hot-sby:  Port is in a hot-standby state.
  down:     Port is down.

Channel Group 3
  Member Ports: 2, Maxports = 16, Protocol: LACP
                        LACP          Port        Port
  Port          Flags   State         Priority    Number
  ------------------------------------------------------
  Gi1/0/4       FA      down          20000       0
  Gi1/0/5       FA      down          20000       0

GA-MLxxTPoE+#
```

This example shows how to display the neighbor information for port-channel 3.

```
GA-MLxxTPoE+#show channel-group channel 3 neighbor

Flag:
  S - Port is requesting Slow LACPDUs   F - Port is requesting fast LACPDU
  A - Port is in active mode            P - Port is in passive mode

Channel Group 3
                Partner                   Partner    Partner    Partner
  Port          System ID                 PortNo     Flags      Port_Pri
  ------------------------------------------------------------------------
  Gi1/0/21      32768,00-50-40-36-3C-00   21         FA         32768
  Gi1/0/22      32768,00-50-40-36-3C-00   22         FA         32768
  Gi1/0/23          0,00-00-00-00-00-00   0          SP         0
  Gi1/0/24          0,00-00-00-00-00-00   0          SP         0

GA-MLxxTPoE+#
```

This example shows how to display the load balance information for all channel groups.

```
GA-MLxxTPoE+#show channel-group load-balance

load-balance algorithm: src-dst-mac

GA-MLxxTPoE+#
```

This example shows how to display the system identifier information.

```
GA-MLxxTPoE+#show channel-group sys-id

System-ID: 32768,00-50-40-34-00-10

GA-MLxxTPoE+#
```

This example shows how to display the summary information for all port-channels.

```
GA-MLxxTPoE+#show channel-group

load-balance algorithm: src-ip
System-ID: 32768,00-50-40-3F-54-1B

Group           Protocol
-----------------------
3               LACP

GA-MLxxTPoE+#
```

4.3 VLAN (Virtual LAN) Commands

VLAN (Virtual LAN) is a function to divide ports of this switch into groups and create multiple virtual LAN environments. As one VLAN corresponds to the broadcast domain, this function allows to improve security by restraining communications between VLANs, as well as reducing traffic on the network. This switch supports many VLANs, including port-based VLAN, IEEE 802.1Q compliant tagged VLAN, MAC-based VLAN, and subnet VLAN.

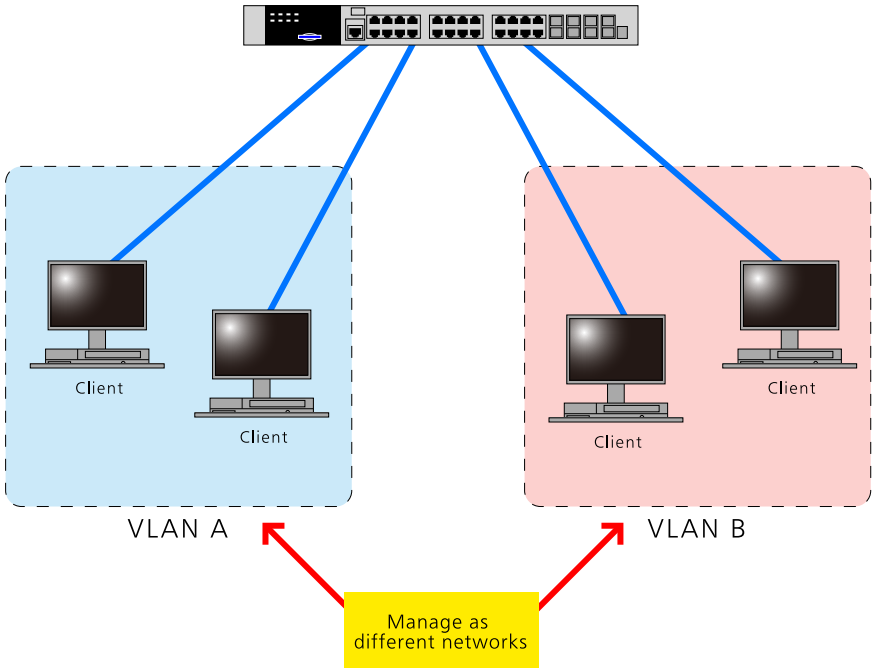


Figure 30-1 VLAN overview

4.3.1 acceptable-frame

This command is used to set the acceptable types of frames by a port. Use the **no** form of this command to revert to the default setting.

Syntax

- **acceptable-frame {tagged-only | untagged-only | admit-all}**
- **no acceptable-frame**

Parameters

Parameters	Description
tagged-only	Specifies that only tagged frames are admitted.
untagged-only	Specifies that only untagged frames are admitted.
admit-all	Specifies that all frames are admitted.

Default

For the access VLAN mode, the default option is **untagged-only**.
For the other VLAN mode, the default option is **admit-all**.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

This command is used to set the acceptable types of frames by a port.

Example

This example shows how to set the acceptable frame type to **tagged-only** for port GigabitEthernet1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# acceptable-frame tagged-only
GA-MLxxTPoE+(config-if)#
```

4.3.2 ingress-checking

This command is used to enable ingress checking for frames received by a port. Use the **no** form of this command to disable the ingress check.

Syntax

- **ingress-checking**
- **no ingress-checking**

Parameters

None

Default

By default, this option is enabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use this command to enable ingress checking for packets received by the interface. If ingress checking is enabled, the packet will be dropped if the received port is not a member port of the VLAN classified for the received packet.

Example

This example shows how to set ingress checking to enabled port GigabitEthernet1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# ingress-checking
GA-MLxxTPoE+(config-if)#
```

4.3.3 mac-vlan

This command is used to create the MAC-based VLAN classification entry. Use the **no** form of this command to remove the MAC-based VLAN classification entry.

Syntax

- **mac-vlan** *MAC-ADDRESS* **vlan** *VLAN-ID* [**priority** *COS-VALUE*]
- **no mac-vlan** *MAC-ADDRESS*

Parameters

Parameters	Description
MAC-ADDRESS	Specifies the MAC address for the entry.
vlan *VLAN-ID*	Specifies the VLAN ID for the MAC-based VLAN entry.
priority *COS-VALUE*	(Optional) Specifies the priority CoS value. If not specified, the default CoS is 0.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use this command to create the MAC-based VLAN classification entry. The classification entry will be applied to packets received by the Switch. By default, the precedence to classify the VLAN for an untagged packet is MAC-based > Subnet-based > Protocol VLAN.

Example

This example shows how to create a MAC-based VLAN ID entry for the MAC address 00-80-cc-00-00-11.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# mac-vlan 00-80-cc-00-00-11 vlan 101 priority 4
GA-MLxxTPoE+(config)#
```

4.3.4 protocol-vlan profile

This command is used to create a protocol group. Use the **no** form of this command to remove the specified protocol group.

Syntax

- **protocol-vlan profile** *PROFILE-ID* **frame-type {ethernet2 | snap | llc} ether-type** *TYPE-VALUE*

- **no protocol-vlan profile** *PROFILE-ID*

Parameters

Parameters	Description
PROFILE-ID	Specifies the protocol group to add or delete.
frame-type	Specifies the frame type.
ethernet2	Specifies the value for the type of the Ethernet II frames.
snap	Specifies the value for the type of the SNAP frames.
llc	Specifies the value for the type of the LLC frames.
ether-type *TYPE-VALUE*	Specifies the type. This value should be 2 bytes in hexadecimal form.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use the **protocol-vlan profile** command in the global configuration mode to create a protocol group. Then use the **protocol-vlan profile** command in the interface configuration mode to configure the VLAN classification for the protocol group received by the port.

Example

This example shows how to create a protocol VLAN group with a group ID of 10, specifying that the IPv6 protocol (frame type is Ethernet2 value is 0x86dd) will be used.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# protocol-vlan profile 10 frame-type ethernet2 ether-type 0x86dd
GA-MLxxTPoE+(config)#
```

4.3.5 protocol-vlan profile (Interface)

This command is used to configure the VLAN classification entry for a protocol group on a port. Use the **no** form of this command to remove the VLAN classification entry on a port.

Syntax

- **protocol-vlan profile** *PROFILE-ID* **vlan** *VLAN-ID* [**priority** *COS-VALUE*]
- **no protocol-vlan profile** *PROFILE-ID*

Parameters

Parameters	Description
PROFILE-ID	Specifies the ID of the protocol group to be classified.
vlan *VLAN-ID*	Specifies the VLAN ID of the protocol VLAN. Only one VLAN ID can be specified for each binding group.
priority *COS-VALUE*	(Optional) Specifies the priority CoS value. If not specified, the default COS is 0.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use this to specify a VLAN for a protocol group on a port. As a result, the packet received by the port that matches the specified protocol group will be classified to the specified VLAN. The VLAN does not need to exist to configure the command. The precedence for classifying the untagged packet is MAC-based > Subnet-based > Protocol VLAN.

Example

This example shows how to create a VLAN classification entry on gi1/0/1 to classify packets in the protocol group 10 to VLAN 3000.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# protocol-vlan profile 10 vlan 3000
GA-MLxxTPoE+(config-if)#
```

4.3.6 subnet-vlan

The **subnet-vlan ipv4** command is used to configure a VLAN classification entry for an IPv4 subnet. The **subnet-vlan ipv6** command is used to configure a VLAN classification entry for an IPv6 subnet. Use the **no** form of this command to remove a subnet-based VLAN classification entry.

Syntax

- **subnet-vlan** {**ipv4** *NETWORK-PREFIX NETWORK-MASK* | **ipv6** *IPV6-NETWORK-PREFIX/PREFIX-LENGTH*} **vlan** *VLAN-ID* [**priority** *COS-VALUE*]
- **no subnet-vlan** {**ipv4** *NETWORK-PREFIX NETWORK-MASK* | **ipv6** *IPV6-NETWORK-PREFIX/PREFIX-LENGTH*}

Parameters

Parameters	Description
ipv4 *NETWORK-PREFIX NETWORK-MASK*	Specifies the IPv4 network prefix and network mask.
ipv6 *IPV6-NETWORK-PREFIX/PREFIX-LENGTH*	Specifies the IPv6 network prefix and the prefix length. The prefix length of IPv6 network address cannot be greater than 64 bits.
vlan *VLAN-ID*	Specifies the VLAN ID of the subnet VLAN.
priority *COS-VALUE*	(Optional) Specifies the priority CoS value. If not specified, the default COS is 0.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use the **subnet-vlan ipv4** command to configure a VLAN classification entry for an IPv4 subnet. Use the **subnet-vlan ipv6** command to configure a VLAN classification entry for an IPv6 subnet. The classification entry will be applied to packets received by the Switch. By default, the precedence to classify the VLAN for an untagged packet is MAC-based > Subnet-based > Protocol VLAN.

Example

This example shows how to configure VLAN classification entries to classify that packets belong to subnets 20.0.0.0/8, 192.0.0.0/8, and 3ffe:22:33:44::/64 to VLAN 100.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# subnet-vlan ipv4 20.0.0.0/8 vlan 100
GA-MLxxTPoE+(config)# subnet-vlan ipv4 192.0.0.0/8 vlan 100 priority 4
GA-MLxxTPoE+(config)# subnet-vlan ipv6 3ffe:22:33:44::/64 vlan 100
GA-MLxxTPoE+(config)#
```

4.3.7 show protocol-vlan profile

This command is used to display the configuration settings of the protocol VLAN related setting.

Syntax

- **show protocol-vlan** {**profile** [*PROFILE-ID* [**,** | **-**]] | **interface** [*INTERFACE-ID* [**,** | **-**]]}

Parameters

Parameters	Description
profile	Specifies the protocol group.
PROFILE-ID	(Optional) Specifies the protocol group to be displayed.
,	(Optional) Specifies a series of profile IDs, or separate a range of profile IDs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of profile IDs. No space is allowed before and after the hyphen.
interface	Specifies the interfaces to be displayed.

Parameters	Description
INTERFACE-ID	(Optional) Specifies the port to display the protocol VLAN classification setting.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guidelines

Use this command to display the settings for VLAN classification on a port based on the protocol group.

Example

This example shows how to display the setting for VLAN classification based on the protocol group on GigabitEthernet1/0/1 to 1/0/3.

```
GA-MLxxTPoE+#show protocol-vlan interface gi1/0/1-3

 Interface       Protocol Group ID  VLAN  Priority
 --------------  -----------------  ----  --------
 Gi1/0/1         10                 3000  0
 Gi1/0/2         10                 3     0
                 11                 2001  4
                 12                 3002  1
 Gi1/0/3         2                  100   6

GA-MLxxTPoE+#
```

This example shows how to display the protocol group profile settings.

```
GA-MLxxTPoE+#show protocol-vlan profile

 Profile ID  Frame-type   Ether-type
 ----------  -----------  ----------------
 1           Ethernet2    0x8600(User define)
 10          Ethernet2    0x86DD(IPv6)

GA-MLxxTPoE+#
```

4.3.8 show vlan

This command is used to display the parameters for all configured VLANs or one VLAN on the Switch.

Syntax

- **show vlan** [*VLAN-ID* [, | -] | **interface** [*INTERFACE-ID* [, | -]] | **mac-vlan** | **subnet-vlan**]

Parameters

Parameters	Description
VLAN-ID	(Optional) Specifies a list of VLANs to display the member port information. If the VLAN is not specified, all VLANs are displayed. The valid range is from 1 to 4094.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.
interface *INTERFACE-ID*	(Optional) Specifies the port to display the VLAN related setting.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
mac-vlan	(Optional) Specifies to display MAC-based VLAN information.
subnet-vlan	(Optional) Specifies to display subnet-based VLAN information.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guidelines

This command is used to display the parameters for all configured VLANs or one VLAN on the Switch.

Example

This example shows how to display all the current VLAN entries.

```
GA-MLxxTPoE+#show vlan

VLAN 1
   Name : default
   Tagged Member Ports   :
   Untagged Member Ports : Gi1/0/1-1/0/10

Total Entries : 1

GA-MLxxTPoE+#
```

This example shows how to display the PVID, ingress checking, and acceptable frame type information for GigabitEthernet1/0/1-1/0/2.

```
GA-MLxxTPoE+# show vlan interface gi1/0/1-1/0/4

 Gi1/0/1
   VLAN Mode              : Hybrid
   Native VLAN            : 1
   Hybrid Untagged VLAN   : 1
   Hybrid Tagged VLAN     :
   Ingress Checking       : Enabled
   Acceptable Frame Type  : Admit-All
   Dynamic Tagged VLAN    :
   VLAN Precedence        : MAC-VLAN

 Gi1/0/2
   VLAN Mode              : Hybrid
   Native VLAN            : 1
   Hybrid Untagged VLAN   : 1
   Hybrid Tagged VLAN     :
   Ingress Checking       : Enabled
   Acceptable Frame Type  : Admit-All
   Dynamic Tagged VLAN    :
   VLAN Precedence        : MAC-VLAN


GA-MLxxTPoE+#
```

This example shows how to display all the MAC−based VLAN entries.

```
GA-MLxxTPoE+# show vlan mac-vlan

 MAC Address          VLAN ID   Priority  Status
 -------------------  --------  --------  ----------
 00-80-cc-00-00-11    101         4       Active

 Total Entries: 1

GA-MLxxTPoE+#
```

This example shows how to display all the subnet−based VLAN entries.

```
GA-MLxxTPoE+# show vlan subnet-vlan

 Subnet                     VLAN ID  Priority
 -------------------------  -------  ---------
 20.0.0.0/8                 100      0
 192.0.0.0/8                100      4
 3FFE:22:33:44::/64         100      0

 Total Entries: 3

GA-MLxxTPoE+#
```

4.3.9 switchport access vlan

This command is used to specify the access VLAN for an interface. Use the **no** form of this command to revert to the default setting.

Syntax

- switchport access vlan *VLAN-ID*
- no switchport access vlan

Parameters

Parameters	Description
VLAN-ID	Specifies the access VLAN of the interface.

Default

By default, this access VLAN is VLAN 1.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

The command takes effect when the interface is set to access mode, or dot1q-tunnel mode. The VLAN specified as the access VLAN does not need to exist to configure the command.
Only one access VLAN can be specified. The succeeding command overwrites the previous command.

Example

This example shows how to configure the GigabitEthernet1/0/1 to access mode with access VLAN 1000.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# switchport mode access
GA-MLxxTPoE+(config-if)# switchport access vlan 1000
GA-MLxxTPoE+(config-if)#
```

4.3.10 switchport hybrid allowed vlan

This command is used to specify the tagged or untagged VLANs for a hybrid port. Use the no form of this command to revert to the default setting.

Syntax

- switchport hybrid allowed vlan {[add] {tagged | untagged} | remove} *VLAN-ID* [, | -]
- no switchport hybrid allowed vlan

Parameters

Parameters	Description
add	(Optional) Specifies the port will be added into the specified VLAN(s).
tagged	Specifies the port as a tagged member of the specified VLAN(s).
untagged	Specifies the port as an untagged member of the specified VLAN(s).
remove	Specifies the port will be removed from the specified VLAN(s).
VLAN-ID	Specified the allowed VLAN list or the VLAN list to be added to or removed from the allow VLAN list. If no option is specified, the specified VLAN list will overwrite the allowed VLAN list.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.

Default

By default, a hybrid port is an untagged member port of VLAN 1.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

By setting the hybrid VLAN command multiple times with different VLAN IDs, a port can be a tagged member port or an untagged member port of multiple VLANs.

When the allowed VLAN is only specified as the VLAN ID, the succeeding command will overwrites the previous command. If the new untagged allowed VLAN list is overlap with the current tagged allowed VLAN list, the overlap part will change to the untagged allowed VLAN. On the other hand, if the new tagged allowed VLAN list is overlap with current untagged allowed VLAN list, the overlap part will change to the tagged allowed VLAN. The last command will take effect. The VLAN does not need to exist to configure the command.

Example

This example shows how to configure gi1/0/1 to be a tagged member of VLAN 1000 and an untagged member of VLAN 2000 and 3000.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# switchport mode hybrid
GA-MLxxTPoE+(config-if)# switchport hybrid allowed vlan add tagged 1000
GA-MLxxTPoE+(config-if)# switchport hybrid allowed vlan add untagged 2000,3000
GA-MLxxTPoE+(config-if)#
```

4.3.11 switchport hybrid native vlan

This command is used to specify the native VLAN ID of a hybrid port. Use the **no** form of this command to revert to the default setting.

Syntax

- **switchport hybrid native vlan** *VLAN-ID*
- **no switchport hybrid native vlan**

Parameters

Parameters	Description
VLAN-ID	Specifies the native VLAN of a hybrid port.

Default

By default, the native VLAN of a hybrid port is VLAN 1.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

When configuring the hybrid port join to its native VLAN, use the **switchport hybrid allowed vlan** command to add the native VLAN into its allowed VLAN. The specified VLAN does not need to exist to apply the command. The command takes effect when the interface is set to hybrid mode.

Example

This example shows how to configure gi1/0/1 to become a hybrid interface and configure the PVID to 20.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# switchport mode hybrid
GA-MLxxTPoE+(config-if)# switchport hybrid allowed vlan add untagged 1000,20
GA-MLxxTPoE+(config-if)# switchport hybrid native vlan 20
GA-MLxxTPoE+(config-if)#
```

4.3.12 switchport mode

This command is used to specify the VLAN mode for the port. Use the **no** form of this command to revert to the default setting.

Syntax

- **switchport mode {access | hybrid | trunk}**
- **no switchport mode**

Parameters

Parameters	Description
access	Specifies the port as an access port.
hybrid	Specifies the port as a hybrid port.
trunk	Specifies the port as a trunk port.

Default

By default, this option is **hybrid**.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

When a port is set to access mode, this port will be an untagged member of the access VLAN configured for the port. When a port is set to hybrid mode, the port can be an untagged or tagged member of all VLANs configured. The purpose of this VLAN mode is to support of protocol VLAN, subnet-based VLAN, and MAC-based VLAN.
When a port is set to trunk mode, this port is either a tagged or untagged member port of its native VLAN and can be a tagged member of other VLANs configured. The purpose of a trunk port is to support the switch-to-switch connection.
When the switch-port mode is changed, the VLAN related setting associated with previous mode will be lost.

NOTE When the switchport mode is **access**, only untagged packets can be forwarded through the MPLS Virtual Circuit (VC). To be able to forward both tagged and untagged packets through the MPLS VC, configure the switchport mode as **trunk**.

Example

This example shows how to set the GigabitEthernet1/0/1 as a trunk port.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# switchport mode trunk
GA-MLxxTPoE+(config-if)#
```

4.3.13 switchport trunk allowed vlan

To establish a VLAN that spans multiple switches, you need to enable VLAN Trunking on ports connecting the switches. In a trunking port, packets with a VLAN tag added are transferred from switch to switch and sent to the VLAN specified by the tag information on the destination switch.

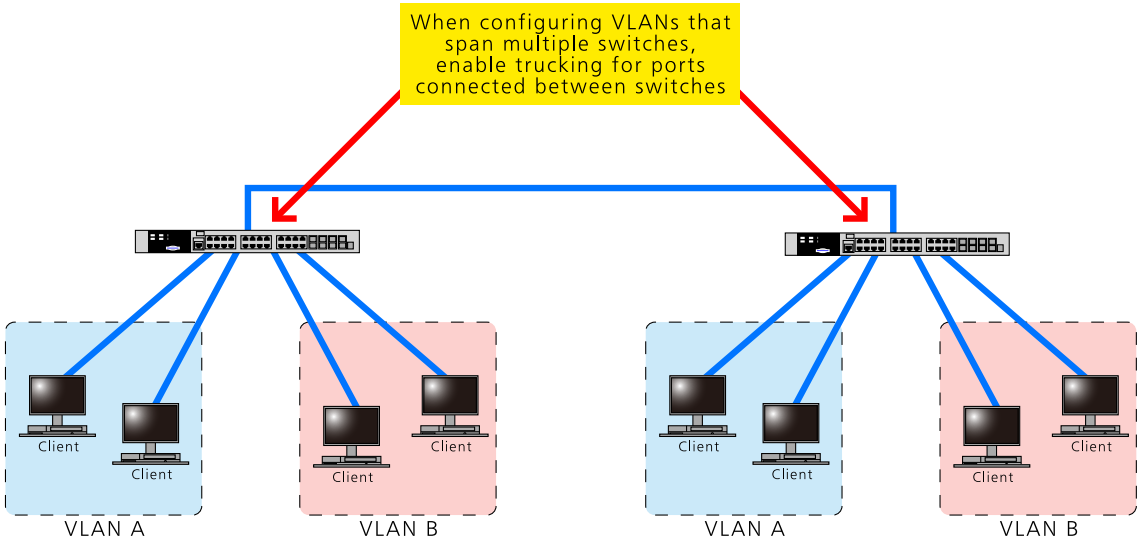


Figure 30-2 VLAN Trunking overview

A trunk interface is an untagged member of a single VLAN, and, in addition, it may be an tagged member of one or more VLANs. Use the **switchport trunk allowed vlan** Interface Configuration mode command to add/remove VLAN(s) to/ from a trunk port. Use the no form of the command to return to the default.

This command is used to configure the VLANs that are allowed to receive and send traffic on the specified interface in a tagged format. Use the **no** form of this command to revert to the default setting.

Syntax

- **switchport trunk allowed vlan** {**all** | [**add** | **remove** | **except**] *VLAN-ID* [**,** | **-**]}
- **no switchport trunk allowed vlan**

Parameters

Parameters	Description
all	Specifies that all VLANs are allowed on the interface.
add	Specifies to add the specified VLAN list to the allowed VLAN list.
remove	Specifies to remove the specified VLAN list from the allowed VLAN list.
except	Specifies that all VLANs except the VLANs in the exception list are allowed.
VLAN-ID	Specifies the allow VLAN list or the VLAN list to be added to or removed from the allow VLAN list.

Parameters	Description
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.

Default

By default, all VLANs are allowed.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

This command only takes effect when the interface is set to trunk mode. If a VLAN is allowed on a trunk port, the port will become the tagged member of the VLAN. When the allowed VLAN option is set to **all**, the port will be automatically added to all the VLAN created by the system.

Example

This example shows how to configure GigabitEthernet1/0/1 as a tagged member of VLAN 1000.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# switchport mode trunk
GA-MLxxTPoE+(config-if)# switchport trunk allowed vlan add 1000
GA-MLxxTPoE+(config-if)#
```

4.3.14 switchport trunk native vlan

This command is used to specify the native VLAN ID of a trunk mode interface. Use the **no** form of this command to revert to the default setting.

Syntax

- **switchport trunk native vlan** { *VLAN-ID* | **tag** }

- no switchport trunk native vlan [tag]

Parameters

Parameters	Description
VLAN-ID	Specifies the native VLAN for a trunk port.
tag	Specifies to enable the tagging mode of the native VLAN.

Default

By default, the native VLAN is 1, untagged mode.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

The command only takes effect when the interface is set to trunk mode. When a trunk port native VLAN is set to tagged mode, normally the acceptable frame type of the port should be set to “tagged-only” to only accept tagged frames. When a trunk port works in the untagged mode for a native VLAN, transmitting untagged packet for a native VLAN and tagged packets for all other VLANs and the acceptable frame types of the port has to be set to “admit-all” in order to function correctly.
The specified VLAN does not need to exist to apply the command.

Example

This example shows how to configure GigabitEthernet1/0/1 as a trunk interface and configures the native VLAN to 20.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# switchport mode trunk
GA-MLxxTPoE+(config-if)# switchport trunk native vlan 20
GA-MLxxTPoE+(config-if)#
```

4.3.15 vlan

This command is used to add VLANs and enter the VLAN configuration mode. Use the **no** form of this command to remove VLANs.

Syntax

- **vlan** *VLAN-ID* [**,** | **-**]
- **no vlan** *VLAN-ID* [**,** | **-**]

Parameters

Parameters	Description
VLAN-ID	Specifies the ID of the VLAN to be added, removed or configured. The valid VLAN ID range is from 1 to 4094. VLAN ID 1 cannot be removed.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.

Default

The VLAN ID 1 exists in the system as the default VLAN.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use the **vlan** global configuration command to create VLANs. Entering the **vlan** command with a VLAN ID enters the VLAN configuration mode. Entering the VLAN ID of an existing VLAN does not create a new VLAN, but allows the user to modify the VLAN parameters for the specified VLAN. When the user enters the VLAN ID of a new VLAN, the VLAN will be automatically created.

Use the **no vlan** command to remove a VLAN. The default VLAN cannot be removed. If the removed VLAN is a port's access VLAN, the port's access VLAN will be reset to VLAN 1.

Example

This example shows how to add new VLANs, assigning the new VLANs with the VLAN IDs 1000 to 1005.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1000-1005
GA-MLxxTPoE+(config-vlan)#
```

4.3.16 vlan precedence

This command is used to specify the VLAN classification precedence for the port. Use the **no** form of this command to reset the VLAN classification precedence for the port.

Syntax

- **vlan precedence {mac-vlan | subnet-vlan}**
- **no vlan precedence**

Parameters

Parameters	Description
mac-vlan	Specifies the port MAC-based VLAN classification is precedence than the subnet-based VLAN.
subnet-vlan	Specifies the port subnet-based VLAN classification is precedence than MAC-based VLAN.

Default

By default, this option is Mac-based VLAN.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

By default, the precedence to classify the VLAN for an untagged packet is MAC-based > Subnet-based > Protocol VLAN. Use the **vlan precedence** command to configure the VLAN classification precedence between MAC-based VLAN and subnet-based VLAN. The command only takes effect on hybrid or dot1q tunnel interfaces.

Example

This example shows how to configure the GigabitEthernet1/0/1 as a subnet VLAN has higher precedence.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# vlan precedence subnet-vlan
GA-MLxxTPoE+(config-if)#
```

4.3.17 name

This command is used to specify the name of a VLAN. Use the **no** form of this command to revert to the default setting.

Syntax

- **name** *VLAN-NAME*
- **no name**

Parameters

Parameters	Description
VLAN-NAME	Specifies the VLAN name, with a maximum of 32 characters. The VLAN name must be unique within the administrative domain.

Default

The default VLAN name is VLANx, where x represents four numeric digits (including the leading zeros) that are equal to the VLAN ID.

Command Mode

VLAN Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use this command to specify the name of a VLAN. The VLAN name must be unique within the administrative domain.

Example

This example shows how to configure the VLAN name of VLAN 1000 to be “admin-vlan”.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1000
GA-MLxxTPoE+(config-vlan)# name admin-vlan
GA-MLxxTPoE+(config-vlan)#
```

4.4 Internet Mansion

Internet mansion is a switch to be used in an Internet mansion, which ensures security easily. The specified port is set as the uplink port and all other ports are set as the downlink ports automatically. The communication between the specified uplink port and each downlink port is enabled, while the communication between downlink ports is disabled. The security of each house is ensured this way.

4.4.1 internet-mansion

The **internet-mansion** command is used to specify the uplink port. Use the **no** form of this command to remove the configuration of Internet mansion.

Syntax

- **internet mansion** interface-id
- **no internet mansion**

Parameters

Parameter	Description
interface-id	Specifies the uplink shared port of Internet mansion.

Default

N/A

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to configure the uplink shared port of Internet mansion. The Internet mansion function and the port grouping function cannot be used at the same time.

Example

This example shows how to configure gi1/0/5 and gi1/0/6 as the uplink port of the Internet mansion.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#internet mansion 5-6
GA-MLxxTPoE+(config)#
```

4.4.2 show vlan

This command is used to display the configuration of Internet mansion, vlan.

Syntax

- show vlan

Parameters

N/A

Default

N/A

Command Mode

Privileged Mode

Command Default Level

Level:1

Usage Guideline

This command is used to display the configuration of Internet mansion.

Example

This example shows how to display the configuration of Internet mansion.

```
GA-MLxxTPoE+#show vlan

 Internet Mansion : Enabled
 UpLink           : 5,6

 VLAN 1
    Name : default
    Tagged Member Ports   :
    Untagged Member Ports : Gi1/0/1-1/0/6

 VLAN 2
    Name : VLAN0002
    Tagged Member Ports   :
    Untagged Member Ports : Gi1/0/1,1/0/5-1/0/6

 VLAN 3
    Name : VLAN0003
    Tagged Member Ports   :
    Untagged Member Ports : Gi1/0/2,1/0/5-1/0/6

 VLAN 4
    Name : VLAN0004
    Tagged Member Ports   :
    Untagged Member Ports : Gi1/0/3,1/0/5-1/0/6

 VLAN 5
    Name : VLAN0005
    Tagged Member Ports   :
    Untagged Member Ports : Gi1/0/4-1/0/6

 Total Entries : 5

GA-MLxxTPoE+#
```

4.5 Port Grouping

Port grouping is a function which enables the communication exclusively between ports which belong to the same group.

4.5.1 port-group

The **port-group** command is used to group the ports. Use the **no** form of this command to remove a port group.

Syntax

- **port-group** group-id {**enable** | {**name** group-name **member** interface-id }}
- **no port-group** group-id

Parameters

Parameter	Description
group-id	Specifies the ID of a port group. The possible values are from 1 to 256.
group-name	Specifies the name of the port group. The possible number of characters is from 1 to 16.
interface-id	Specifies ports which belong to the port group.

Default

N/A

Command Mode

Global Configuration Mode

Command Default Level

Level:12

Usage Guideline

This command is used to configure a port group. The port grouping function and the Internet mansion function cannot be used at the same time.

Example

This example shows how to configure ports gi1/0/3 and gi1/0/4 to the port group 1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#port-group 1 name group1 member 3-4
GA-MLxxTPoE+(config)#
```

4.5.2 show port-group

This command is used to display the configuration of port grouping.

Syntax

- show port-group

Parameters

N/A

Default

N/A

Command Mode

Privileged Mode

Command Default Level

Level:1

Usage Guideline

This command is used to display the configuration of port grouping function.

Example

This example shows how to display the configuration of port grouping function.

```
GA-MLxxHPoE+#show port-group

 Group ID  Group Name          Group Member                                 Status
 --------  ----------------  ------------------------------------------  --------
     1     group1            Gi1/0/3-1/0/4                               Enabled

 Total Groups : 1

GA-MLxxHPoE+#
```

4.6 Private VLAN Commands

4.6.1 private-vlan

This command is used to configure a VLAN as a private VLAN. Use the **no** form of this command to remove the private VLAN configuration.

Syntax

- **private-vlan {community | isolated | primary}**
- **no private-vlan {community | isolated | primary}**

Parameters

Parameters	Description
community	Specifies the VLAN as a community VLAN in a private VLAN domain. Member ports within a community VLAN can communicate with each other but cannot communicate with member ports of other communities at Layer 2.
isolated	Specifies the VLAN as an isolated VLAN in a private VLAN domain. Member ports of an isolate VLAN cannot communicate with each other and with member ports of the community VLAN at Layer 2.
primary	Specifies the VLAN as a primary VLAN in a private VLAN domain.

Default

None

Command Mode

VLAN Configuration Mode

Command Default Level

Level: 12

Usage Guideline

A private VLAN domain is defined with one primary VLAN, one isolated VLAN, and multiple community VLANs. Use this command first to specify the role of the private VLAN before they can be referenced in other private VLAN configuration commands.

Example

This example shows how to configure a VLAN as a private VLAN. VLAN 1000, VLAN 1001 and VLAN 1002 are configured as a primary VLAN, an isolated VLAN and a community VLAN respectively.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1000
GA-MLxxTPoE+(config-vlan)# private-vlan primary
GA-MLxxTPoE+(config-vlan)# exit
GA-MLxxTPoE+(config)# vlan 1001
GA-MLxxTPoE+(config-vlan)# private-vlan isolated
GA-MLxxTPoE+(config-vlan)# exit
GA-MLxxTPoE+(config)# vlan 1002
GA-MLxxTPoE+(config-vlan)# private-vlan community
GA-MLxxTPoE+(config-vlan)#
```

4.6.2 private-vlan association

This command is used to associate secondary VLANs with a primary VLAN. Use the **no** form of this command to remove the association of secondary VLANs with the primary VLAN.

Syntax

- **private-vlan association** {**add** *SECONDARY-VLAN-ID* [**,** | **-**] | **remove** *SECONDARY-VLAN-ID* [**,** | **-**]}
- **no private-vlan association**

Parameters

Parameters	Description
add *SECONDARY-VLAN-ID*	Specifies to add the association of the specified secondary VLANs with the primary VLAN. The valid ID range of secondary VLAN is from 2 to 4094.
remove *SECONDARY-VLAN-ID*	Specifies to remove the association of the specified secondary VLANs with the primary VLAN.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.

Parameters	Description
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.

Default

None

Command Mode

VLAN Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Only one isolated VLAN can be associated with the primary VLAN. Multiple community VLANs can be associated with the primary VLAN. A secondary VLAN can only be associated with one primary VLAN.

Example

This example shows how to associate secondary VLAN 1001 and secondary VLAN 1002 with the primary VLAN 1000.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1000
GA-MLxxTPoE+(config-vlan)# private-vlan association add 1001-1002
GA-MLxxTPoE+(config-vlan)#
```

4.6.3 private-vlan synchronize

This command is used to synchronize secondary VLANs to have the same mapping MST ID as the primary VLAN.

Syntax

- private-vlan synchronize

Parameters

None

Default

None

Command Mode

MST Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The secondary VLANs need to be mapped to the same MST ID as the primary VLAN if private VLAN is configured. If the mapping is not synchronized when the user exits the MST Configuration Mode, a warning message will be displayed. Use the **private-vlan synchronize** command to synchronize the MST ID mapping before exiting the MST Configuration Mode. This command will not be saved in the running configuration.

Example

This example shows how to synchronize the MST mapping before exiting the MST Configuration Mode.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# spanning-tree mst configuration
GA-MLxxTPoE+(config-mst)# instance 1 vlans 1-100
GA-MLxxTPoE+(config-mst)# instance 2 vlans 101-200
GA-MLxxTPoE+(config-mst)# private-vlan synchronize
GA-MLxxTPoE+(config-mst)#
```

4.6.4 switchport mode private-vlan

This command is used to specify a port as a private VLAN port. The port type can be a host port, promiscuous port, trunk promiscuous port or trunk secondary port.

Syntax

- **switchport mode private-vlan {host | promiscuous}**

Parameters

Parameters	Description
host	Specifies the port as an isolated port or a community port.
promiscuous	Specifies the port as a promiscuous port.

Default

By default, this option is configured as Hybrid VLAN mode.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

For isolated ports or community ports, use the **switchport mode private-vlan host** command to specify the port mode with the primaryVLAN.
For a promiscuous port, use the **switchport mode private-vlan promiscuous** command to specify the port mode and use the **switchport private-vlan mapping** command to associate the port with a primary VLAN and define the mapping secondary VLAN.
For a trunk port of a primary VLAN, use the **switchport mode trunk** command to specify the port mode and use the **switchport trunk allowed vlan** command to define the associated VLANs.
When an interface's mode is changed, the setting associated with the previous mode will be lost.

Example

This example shows how to configure physical ports as private VLAN ports. Here, we specify the GigabitEthernet1/0/1 as a private VLAN host port and specify the GigabitEthernet1/0/2 as a private VLAN promiscuous port.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# switchport mode private-vlan host
GA-MLxxTPoE+(config-if)# exit
GA-MLxxTPoE+(config)# interface gi1/0/2
GA-MLxxTPoE+(config-if)# switchport mode private-vlan promiscuous
GA-MLxxTPoE+(config-if)#
```

4.6.5 switchport private-vlan host-association

This command is used to associate the private VLAN with an isolated port or a community port. Use the no form of this command to remove the association.

Syntax

- switchport private-vlan host-association *PRIMARY-VLAN-ID SECONDARY-VLAN-ID*
- no switchport private-vlan host-association

Parameters

Parameters	Description
PRIMARY-VLAN-ID	Specifies the ID of primary VLAN to be associated. The valid ID range of a primary VLAN is from 2 to 4094.
SECONDARY-VLAN-ID	Specifies the ID of secondary VLAN to be associated. The valid ID range of a secondary VLAN is from 2 to 4094.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The port is an isolated port if the secondary VLAN specified by the command is an isolated VLAN. The port is a community port if the secondary VLAN specified by the command is a community VLAN.

Example

This example shows how to associate GigabitEthernet1/0/1 with the primary VLAN 1000 and the secondary VLAN 1001.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# switchport mode private-vlan host
GA-MLxxTPoE+(config-if)# switchport private-vlan host-association 1000 1001
GA-MLxxTPoE+(config-if)#
```

4.6.6 switchport private-vlan mapping

This command is used to associate the private VLAN membership with a promiscuous port. Use the **no** form of this command to remove the association.

Syntax

- **switchport private-vlan mapping** *PRIMARY-VLAN-ID* {**add** *SECONDARY-VLAN-ID* [**,** | **-**] | **remove** *SECONDARY-VLAN-ID* [**,** | **-**]}
- **no switchport private-vlan mapping**

Parameters

Parameters	Description
PRIMARY-VLAN-ID	Specifies the primary VLAN to be mapped. The valid ID range of the primary VLAN is from 2 to 4094.
add *SECONDARY-VLAN-ID*	Specifies to add membership of the specified secondary VLAN. The valid ID range of secondary VLAN is from 2 to 4094.
remove *SECONDARY-VLAN-ID*	Specifies to remove membership of the specified secondary VLAN.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command is available for physical port and port-channel interface configuration.

Example

This example shows how to configure GigabitEthernet1/0/2 as a private VLAN promiscuous port and to map it to a primary VLAN 1000 and secondary VLAN 1001 and VLAN 1002.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/2
GA-MLxxTPoE+(config-if)# switchport mode private-vlan promiscuous
GA-MLxxTPoE+(config-if)# switchport private-vlan mapping 1000 add 1001,1002
GA-MLxxTPoE+(config-if)#
```

4.6.7 show vlan private-vlan

This command is used to display private VLAN configurations.

Syntax

- show vlan private-vlan

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command displays the listing of the private VLAN contained in the private VLAN domain, association of a secondary VLAN with a primary VLAN, and member port of each private VLAN.

Example

This example shows how to display the private VLAN settings. In this example, there are two private VLAN domains configured.

```
GA-MLxxTPoE+#show vlan private-vlan

Primary VLAN   Secondary VLAN   Type         Interface
-------------  ---------------  -----------  ----------------------------
1000           1001             Isolated     Gi1/0/1-1/0/2
1000           1002             Community    Gi1/0/2

 Total Entries : 2

GA-MLxxTPoE+#
```

4.7 Asymmetric VLAN Commands

4.7.1 asymmetric-vlan

This command is used to enable the asymmetric VLAN function. Use the **no** form of this command to disable the function.

Syntax

- **asymmetric-vlan**
- **no asymmetric-vlan**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to enable or disable the asymmetric VLAN function.

Example

This example shows how to enable asymmetric VLAN.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)# asymmetric-vlan
GA-MLxxTPoE+(config)#
```

4.8 Voice VLAN Commands

Voice VLAN is a function to configure a voice-specific VLAN to secure the bandwidth of voice data when normal communication data and voice data such as an IP phone coexist on the network. It prevents voice data delay and maintains the quality at the constant level regardless of the traffic status on the network. To use a voice VLAN, you need to pre-register the vendor code (OUI) of an IP phone connected.

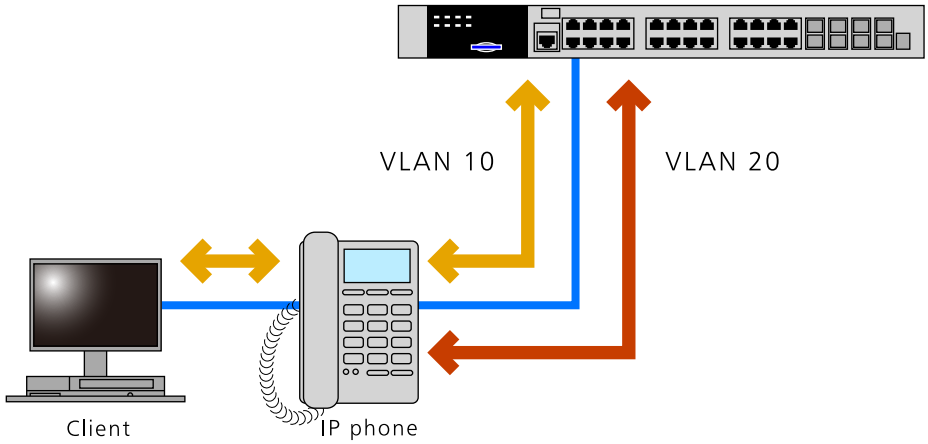


Figure 35-1 Voice VLAN overview

4.8.1 voice vlan

This command is used to enable the global voice VLAN state and configure the voice VLAN. Use the **no** form of this command to disable the voice VLAN state.

Syntax

- **voice vlan** *VLAN-ID*
- **no voice vlan**

Parameters

Parameters	Description
VLAN-ID	Specifies the ID of the voice VLAN. The valid range is from 2 to 4094.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to enable the global voice VLAN function and to specify the voice VLAN on the Switch. The Switch has only one voice VLAN.
Both the **voice vlan** command in the global configuration and the **voice vlan enable** command in the interface configuration mode need to be enabled for a port to start the voice VLAN function.
When the voice VLAN is enabled for a port, the received voice packets will be forwarded in the voice VLAN. The received packets are determined as voice packets if the source MAC addresses of packets comply with the organizationally unique identifier (OUI) addresses configured by the **voice vlan mac-address** command.
The VLAN to be specified as the voice VLAN needs to pre-exist before configuration. If the voice VLAN is configured, the voice VLAN cannot be removed with the **no vlan** command.

Example

This example shows how to enable the voice VLAN function and configure VLAN 1000 as the voice VLAN.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# voice vlan 1000
GA-MLxxTPoE+(config)#
```

4.8.2 voice vlan aging

This command is used to configure the aging time for aging out the voice VLAN's dynamic member ports. Use the **no** form of this command to revert to the default setting.

Syntax

- voice vlan aging *MINUTES*
- no voice vlan aging

Parameters

Parameters	Description
MINUTES	Specifies the aging time of the voice VLAN. The valid range is from 1 to 65535 minutes.

Default

By default, this value is 720 minutes.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to configure the aging time for aging out the voice device and the voice VLAN automatically learned member ports. When the last voice device connected to the port stops sending traffic and the MAC address of this voice device is aged out from FDB, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after the expiration of the voice VLAN aging timer. If voice traffic resumes during the aging time, the aging timer will be cancelled.

Example

This example shows how to configure the aging time of the voice VLAN to 30 minutes.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# voice vlan aging 30
GA-MLxxTPoE+(config)#
```

4.8.3 voice vlan enable

This command is used to enable the voice VLAN state of ports. Use the **no** form of this command to disable the voice VLAN's port state.

Syntax

- **voice vlan enable**
- **no voice vlan enable**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command takes effect for access ports or hybrid ports. Use the **voice vlan enable** command to enable the voice VLAN function for ports. Both the **voice vlan** command in the global configuration and the **voice vlan enable** command in the interface configuration mode need to be enabled for a port to start the voice VLAN function.

Example

This example shows how to enable the voice VLAN function on the physical port GigabitEthernet1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# voice vlan enable
GA-MLxxTPoE+(config-if)#
```

4.8.4 voice vlan mac-address

This command is used to add the user-defined voice device OUI. Use the **no** form of this command to delete the user-defined voice device OUI.

Syntax

- **voice vlan mac-address** *MAC-ADDRESS MASK* [**description** *TEXT*]
- **no voice vlan mac-address** *MAC-ADDRESS MASK*

Parameters

Parameters	Description
MAC-ADDRES	Specifies the OUI MAC address.
MASK	Specifies the OUI MAC address matching bitmask.
description *TEXT*	(Optional) Specifies the description for the user defined OUI with a maximum of 32 characters.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to add a user-defined OUI for the voice VLAN. The OUI for the voice VLAN is used to identify the voice traffic by using the voice VLAN function. If the source MAC addresses of the received packet matches any of the OUI patterns, the received packet is determined as a voice packet.
The user-defined OUI cannot be the same as the default OUI. The default OUI cannot be deleted.

Example

This example shows how to add a user-defined OUI for voice devices.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# voice vlan mac-address 00-02-03-00-00-00 FF-FF-FF-00-00-00
description User1
GA-MLxxTPoE+(config)#
```

4.8.5 voice vlan mode

This command is used to enable the automatic learning of the port as voice VLAN member ports. Use the **no** form of this command to disable the automatic learning.

Syntax

- **voice vlan mode {manual | auto {tag | untag}}**
- **no voice vlan mode**

Parameters

Parameters	Description
manual	Specifies that voice VLAN membership will be manually configured.
auto	Specifies that voice VLAN membership will be automatically learned.
tag	Specifies to learn voice VLAN tagged members.
untag	Specifies to learn voice VLAN untagged members.

Default

By default, this option is set to **untag** and **auto**.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to configure automatic learning or manual configuration of voice VLAN member ports.

If auto-learning is enabled, the port will automatically be learned as a voice VLAN member. This membership will be automatically be aged out. When the port is working in the **auto tagged** mode and the port captures a voice device through the device's OUI, it will join the voice VLAN as a tagged member automatically. When the voice device sends tagged packets, the Switch will change its priority. When the voice device sends untagged packets, it will forward them in port's PVID VLAN.
When the port is working in **auto untagged** mode, and the port captures a voice device through the device's OUI, it will join the voice VLAN as an untagged member automatically. When the voice device sends tagged packets, the Switch will change its priority. When the voice device sends untagged packets, it will forward them in voice VLAN.
When the Switch receives LLDP-MED packets, it checks the VLAN ID, tagged flag, and priority flag. The Switch should follow the tagged flag and priority setting.
If auto learning is disabled, the user should use the **switchport hybrid vlan** command to configure the port as a voice VLAN tagged or untagged member port.

Example

This example shows how to configure physical port GigabitEthernet1/0/1 to be in the **auto tag** mode.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# voice vlan mode auto tag
GA-MLxxTPoE+(config-if)#
```

4.8.6 voice vlan qos

This command is used to configure the CoS priority for the incoming voice VLAN traffic. Use the **no** form of this command to revert to the default setting.

Syntax

- **voice vlan qos** *COS-VALUE*
- **no voice vlan qos**

Parameters

Parameters	Description
COS-VALUE	Specifies the priority of the voice VLAN. This value must be between 0 and 7.

Default

By default, this value is 5.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The voice packets arriving at the voice VLAN enabled port are marked to the CoS specified by the command. The remarking of CoS allows the voice VLAN traffic to be distinguished from data traffic in quality of service.

Example

This example shows how to configure the priority of the voice VLAN to be 7.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# voice vlan qos 7
GA-MLxxTPoE+(config)#
```

4.8.7 show voice vlan

This command is used to display the voice VLAN configurations.

Syntax

- **show voice vlan [interface [***INTERFACE-ID* **[, | -]]]**
- **show voice vlan {device | lldp-med device} [interface** *INTERFACE-ID* **[, | -]]**

Parameters

Parameters	Description
interface *INTERFACE-ID*	(Optional) Specifies to display voice VLAN information of ports.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Parameters	Description
device	Specifies to display the voice devices learned by OUI.
lldp-med device	Specifies to display the voice devices learned by LLDP-MED.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command is used to display the voice VLAN configurations.

Example

This example shows how to display the voice VLAN global settings.

```
GA-MLxxTPoE+#show voice vlan

 Voice VLAN ID        : 1000
 Voice VLAN CoS       : 5
 Aging Time           : 30 minutes
 Member Ports         :
 Dynamic Member Ports :

 Voice VLAN OUI       :

 OUI Address        Mask               Description
 -----------------  -----------------  --------------

 Total OUI: 0

GA-MLxxTPoE+#
```

This example shows how to display the voice VLAN information of ports.

```
GA-MLxxTPoE+#show voice vlan interface gi 1/0/1-3

 Interface       State     Mode
 --------------  --------  -----------
 Gi1/0/1         Enabled   Auto/Tag
 Gi1/0/2         Disabled  Auto/Untag
 Gi1/0/3         Disabled  Auto/Untag

GA-MLxxTPoE+#
```

This example shows how to display the learned voice devices on ports GigabitEthernet1/0/1-1/0/2.

```
GA-MLxxTPoE+#show voice vlan device interface gi1/0/1-2

 Interface       Voice Device       Start Time         Status
 --------------  -----------------  -----------------  ------
 Gi1/0/1         00-03-6B-00-00-01  2017-03-19 09:00   Active
 Gi1/0/1         00-03-6B-00-00-02  2017-03-20 10:09   Aging
 Gi1/0/1         00-03-6B-00-00-05  2017-03-20 12:04   Active
 Gi1/0/2         00-03-6B-00-00-0a  2017-03-19 08:11   Aging
 Gi1/0/2         33-00-61-10-00-11  2017-03-20 06:45   Aging

Total Entries: 5

GA-MLxxTPoE+#
```

This example shows how to display the learned LLDP-MED voice devices on ports GigabitEthernet1/0/1-1/0/2.

```
GA-MLxxTPoE+#show voice vlan lldp-med device interface gi1/0/1-2

 Index              : 1
 Interface          : Gi1/0/1
 Chassis ID Subtype : MAC Address
 Chassis ID         : 00-E0-BB-00-00-11
 Port ID Subtype    : Network Address
 Port ID            : 172.18.1.1
 Create Time        : 2/23/2017  05:21:14
 Remain Time        : 108 Seconds

 Index              : 2
 Interface          : Gi1/0/2
 Chassis ID Subtype : MAC Address
 Chassis ID         : 00-E0-BB-00-00-12
 Port ID Subtype    : Network Address
 Port ID            : 172.18.1.2
 Create Time        : 2/23/2017  05:21:14
 Remain Time        : 105 Seconds

 Total Entries: 2

GA-MLxxTPoE+#
```

4.9 GVRP (GARP VLAN Registration Protocol) Commands

4.9.1 clear gvrp statistics

This command is used to clear the statistics for a GVRP port.

Syntax

- **clear gvrp statistics** {**all** | **interface** *INTERFACE-ID* [**,** | **-**]}

Parameters

Parameters	Description
all	Specifies to clear GVRP statistic counters associated with all interfaces.
interface *INTERFACE-ID*	Specifies the interfaces to be configured.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to clear the GVRP counters.

Example

This example shows how to clear statistics for all interfaces.

```
GA-MLxxTPoE+# clear gvrp statistics all
GA-MLxxTPoE+#
```

4.9.2 gvrp global

This command is used to enable the GVRP function globally. Use the **no** form of this command to disable the GVRP function globally.

Syntax

- **gvrp global**
- **no gvrp global**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Administrators can enable the global GVRP state and individual port's GVRP state to start GVRP on the port.

Example

This example shows how to enable the GVRP protocol global state.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# gvrp global
GA-MLxxTPoE+(config)#
```

4.9.3 gvrp enable

This command is used to enable the GVRP function on a port. Use the **no** form of this command to disable the GVRP function on a port.

Syntax

- **gvrp enable**
- **no gvrp enable**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is available for both physical ports and port-channel interface configuration. This command only takes effect for hybrid mode and trunk mode. This command does not take effect if the Layer 2 protocol tunnel is enabled for GVRP.

Example

This example shows how to enable the GVRP function on GigabitEthernet1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# gvrp enable
GA-MLxxTPoE+(config-if)#
```

4.9.4 gvrp advertise

This command is used to specify the VLAN that are allowed to be advertised by the GVRP protocol. Use the **no** form of this command to disable the VLAN advertisement function.

Syntax

- **gvrp advertise** {**all** | [**add** | **remove**] *VLAN-ID* [**,** | **-**]}
- **no gvrp advertise**

Parameters

Parameters	Description
all	Specifies that all VLANs are advertised on the interface.
add	(Optional) Specifies a VLAN or a list VLANs to be added to advertise the VLAN list.
remove	(Optional) Specifies a VLAN or a list VLANs to be removed from the advertised VLAN list.
VLAN-ID	Specified the VLAN ID to be added to or removed from the advertise VLAN list. If the **add** or **remove** parameter is not specified, the specified VLAN list overwrites the advertise VLAN list. The range is from 1 to 4094.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.

Default

By default, no VLANs are advertised.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command is available for both physical ports and port-channel interface configuration. Administrators can use the **gvrp advertise** command to enable the specified VLANs' GVRP advertise function on the specified interface. The command only takes effect when GVRP is enabled. The command only takes effect for hybrid mode and trunk mode.

Example

This example shows how to enable the advertise function of VLAN 1000 on GigabitEthernet1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# gvrp advertise 1000
GA-MLxxTPoE+(config-if)#
```

4.9.5 gvrp vlan create

This command is used to enable dynamic VLAN creation. Use the **no** form of this command to disable the dynamic VLAN creation function.

Syntax

- **gvrp vlan create**
- **no gvrp vlan create**

Parameters

None

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

When dynamic VLAN creation is enabled, if a port has learned a new VLAN membership and the VLAN does not exist, the VLAN will be created automatically. Otherwise, the newly learned VLAN will not be created.

Example

This example shows how to enable the creation of dynamic VLANs registered with the GVRP protocol.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# gvrp vlan create
GA-MLxxTPoE+(config)#
```

4.9.6 gvrp forbidden

This command is used to specify a port as being a forbidden member of the specified VLAN. Use the **no** form of this command to remove the port as a forbidden member of all VLANs.

Syntax

- **gvrp forbidden** {**all** | [**add** | **remove**] *VLAN-ID* [**,** | **-**]}
- **no gvrp forbidden**

Parameters

Parameters	Description
all	Specifies that all VLANs, except VLAN 1, are forbidden on the interface.
add	(Optional) Specifies a VLAN or a list of VLANs to be added to the forbidden VLAN list.
remove	(Optional) Specifies a VLAN or a list of VLANs to be removed from the forbidden VLAN list.
VLAN-ID	Specified the forbidden VLAN list. If the **add** or **remove** parameter is not specified, the specified VLAN list will overwrite the forbidden VLAN list. The range is 2 to 4094.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.

Default

No VLANs are forbidden.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command is available for both physical ports and port-channel interface configuration. As a forbidden port of a VLAN, a port is forbidden from becoming a member port of the VLAN via the GVRP operation. The VLAN specified by the command does not need to exist.
This command only affects the GVRP operation. The setting only takes effect when GVRP is enabled. The command only takes effect for hybrid mode and trunk mode.

Example

This example shows how to configure the GigabitEthernet1/0/1 as a forbidden port of VLAN 1000 via the GVRP operation.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# gvrp forbidden 1000
GA-MLxxTPoE+(config-if)#
```

4.9.7 gvrp timer

This command is used to configure the GVRP timer value on a port. Use the **no** form of the command to revert the timer to the default setting.

Syntax

- **gvrp timer [join** *TIMER-VALUE*] [**leave** *TIMER-VALUE*] [**leave-all** *TIMER-VALUE*]
- **no gvrp timer [join] [leave] [leave-all]**

Parameters

Parameters	Description
join	(Optional) Specifies to set the timer for joining a group. The unit is in a hundredth of a second.
leave	(Optional) Specifies to set the timer for leaving a group. The unit is in a hundredth of a second.
leave-all	(Optional) Specifies to set the timer for leaving all groups. The unit is in a hundredth of a second.
TIMER-VALUE	(Optional) Specifies the timer value in a hundredth of a second. The valid range is 10 to 10000.

Default

Join: 20.
Leave: 60.
Leave-all: 1000.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to configure the GVRP timer value on a port.

Example

This example shows how to configure the leave-all timer to 500 hundredths of a second on GigabitEthernet1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# gvrp timer leave-all 500
GA-MLxxTPoE+(config-if)#
```

4.9.8 show gvrp configuration

This command is used to display the GVRP settings.

Syntax

- show gvrp configuration [interface [*INTERFACE-ID* [, | -]]]

Parameters

Parameters	Description
interface	(Optional) Specifies to display the GVRP interface configuration. If the interface ID is not specified, all interfaces are displayed.
INTERFACE-ID	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command only displays GVRP related configurations. If no parameter is specified, the GVRP global configuration is displayed.

Example

This example shows how to display the GVRP configuration for the global configuration.

```
GA-MLxxTPoE+# show gvrp configuration

 Global GVRP State     : Enabled
 Dynamic VLAN Creation : Enabled

GA-MLxxTPoE+#
```

This example shows how to display the GVRP configuration on interfaces GigabitEthernet1/0/5 to 1/0/6.

```
GA-MLxxTPoE+# show gvrp configuration interface gi1/0/5-1/0/6

 Gi1/0/5
   GVRP Status      : Enabled
   Join Time        : 20 centiseconds
   Leave Time       : 60 centiseconds
   Leave-All Time   : 1000 centiseconds
   Advertise VLAN   : 1-4094
   Forbidden VLAN   : 2

 Gi1/0/6
   GVRP Status      : Disabled
   Join Time        : 20 centiseconds
   Leave Time       : 60 centiseconds
   Leave-All Time   : 1000 centiseconds
   Advertise VLAN   :
   Forbidden VLAN   :


GA-MLxxTPoE+#
```

4.9.9 show gvrp statistics

This command is used to display the statistics for a GVRP port.

Syntax

- **show gvrp statistics [interface** *INTERFACE-ID* **[, | -]]**

Parameters

Parameters	Description
interface *INTERFACE-ID*	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

User EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command only displays the ports which have the GVRP state enabled.

Example

This example shows how to display statistics for GVRP interfaces GigabitEthernet1/0/5 to 1/0/6.

```
GA-MLxxTPoE+#show gvrp statistics interface gi1/0/5-1/0/6

 Interface      JoinEmpty  JoinIn     LeaveEmpty LeaveIn   LeaveAll   Empty
 ------------------------------------------------------------------------------
 Gi1/0/5    RX 0          0          0          0         0          0
            TX 4294967296 4294967296 4294967296 429496729642949672964294967296
 Gi1/0/6    RX 0          0          0          0         0          0
            TX 0          0          0          0         0          0

GA-MLxxTPoE+#
```

4.10 NLB (Network Load Balancing) Commands

4.10.1 nlb unicast-fdb

This command is used to add a unicast MAC entry to the NLB unicast address table. Use the **no** form of this command to remove a unicast entry from the NLB unicast address table or remove interfaces from an NLB entry.

Syntax

- **nlb unicast-fdb** *MAC-ADDR* **interface** *INTERFACE-ID* [**,** | **-**]
- **no nlb unicast-fdb** *MAC-ADDR* [**interface** *INTERFACE-ID* [**,** | **-**]]

Parameters

Parameters	Description
MAC-ADDR	Specifies the MAC address of the entry. The address must be a unicast address. If a received packet contains a destination MAC address that matches the specified MAC address, it will be forwarded to the specified interface.
interface *INTERFACE-ID*	Specifies the interface to which the matched packets will be forwarded. Only physical ports are valid interfaces.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to create an NLB unicast MAC entry. The Network Load Balancing (NLB) function is used to support the Microsoft server load balancing application where multiple servers can share the same IP address and MAC address. The requests from clients will be forwarded to all the servers, but will only be processed by one of them. The server can work in two different modes:

- Unicast mode: The client uses a unicast MAC address as the destination MAC address to reach the server.
- Multicast mode: The client uses a multicast MAC address as the destination MAC address to reach the server.

This destination MAC address is called the shared MAC address. However, the server uses its own MAC address (rather than the shared MAC address) as the source MAC address in the reply packet. In other words, a NLB unicast address usually is not the source MAC address of a packet.
When the received packet contains the destination MAC address matches the configured unicast MAC address, it will be forwarded to those configured ports, regardless of the VLAN membership configuration.
Administrators cannot configure a static address of the MAC address table as a NLB address. However, if a MAC address is created as a NLB MAC address entry, the same MAC address can be still dynamically learnt in the Layer 2 MAC address table. In this situation, the NLB has higher priority; the dynamically learnt FDB entry won't take effect.

Example

This example shows how to add an NLB unicast address 00-F3-22-0A-12-F4 to the MAC address table. The candidate forwarding interfaces are GigabitEthernet1/0/1 to 1/0/5.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# nlb unicast-fdb 00-F3-22-0A-12-F4 interface gi1/0/1-5
GA-MLxxTPoE+(config)#
```

4.10.2 nlb multicast-fdb

This command is used to add an entry to the NLB multicast address table. Use the no form of this command to remove an NLB entry from the NLB multicast address table or remove interfaces from a multicast NLB entry.

Syntax

- **nlb multicast-fdb** *MAC-ADDR* **vlan** *VLAN-ID* **interface** *INTERFACE-ID* [**,** | **-**]
- **no nlb multicast-fdb** *MAC-ADDR* **vlan VLAN-ID [interface** *INTERFACE-ID* [**,** | **-**]]

Parameters

Parameters	Description
MAC-ADDR	Specifies the MAC address of the entry. The address must be a multicast address. If a received packet contains a destination address that matches the specified MAC address it will be forwarded to the specified interfaces.
vlan *VLAN-ID*	Specifies the VLAN ID of the entry. The range is from 1 to 4094.
interface *INTERFACE-ID*	Specifies the interface to which the matched packets will be forwarded to. Only physical ports are valid interfaces.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to create an NLB multicast MAC address entry. This destination MAC address is called the shared MAC address. The server uses its own MAC address (rather than the shared MAC) as the source MAC address of the reply packet. In other words, an NLB unicast address usually is not the source MAC address of a packet.

The NLB multicast and Layer 2 multicast FDB are mutually exclusive. The IPv6 multicast mapped MAC addresses (33:33:xx:xx:xx:xx) and IEEE reserved MAC addresses (01:80:c2:00:00:xx) are forbidden to set as the NLB multicast MAC address. NLB entry 01:00:5E:xx:xx:xx (IPv4 multicast mapped MAC address) has higher priority.

Example

This example shows how to add a multicast address 01-F3-22-0A-12-F4 received on VLAN 1 candidate forwarding ports GigabitEthernet1/0/1 to 1/0/5 to the NLB multicast address table.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# nlb multicast-fdb 01-F3-22-0A-12-F4 vlan 1 interface gi1/0/1-5
GA-MLxxTPoE+(config)#
```

4.10.3 show nlb fdb

This command is used to display NLB caonfigured entries.

Syntax

- **show nlb fdb**

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command is used to display NLB configured entries, including unicast and multicast entries.

Example

This example shows how to display NLB configured entries, including unicast and multicast entries.

```
GA-MLxxTPoE+#show nlb fdb

 MAC Address       VLAN ID    Interface
 ----------------- ---------- -------------------------------------------------
 00-F3-22-0A-12-F4 -          Gi1/0/1-1/0/5
 01-F3-22-0A-12-F4 1          Gi1/0/1-1/0/5

Total Entries :2

GA-MLxxTPoE+#
```

4.11 L2PT (Layer 2 Protocol Tunnel) Commands

4.11.1 clear l2protocol-tunnel counters

This command is used to clear the Layer 2 Protocol Tunnel (L2PT) statistics counters.

Syntax

- **clear l2protocol-tunnel counters** {**all** | **interface** *INTERFACE-ID*}

Parameters

Parameters	Description
all	Specifies to clear counters for all interfaces.
interface *INTERFACE-ID*	Specifies the interface to clear counters.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to clear protocol tunnel counters for all interfaces or for the specified interface. Only the physical port and port-channel interface can be specified for the command.

Example

This example shows how to clear L2PT counters for all L2PT ports.

```
GA-MLxxTPoE+# clear l2protocol-tunnel counters all
GA-MLxxTPoE+#
```

4.11.2 l2protocol-tunnel

This command is used to enable the protocol tunneling for the specified protocols. Use the **no** form of this command to disable the protocol tunneling.

Syntax

- **l2protocol-tunnel [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}]**
- **no l2protocol-tunnel [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}]**

Parameters

Parameters	Description
gvrp	(Optional) Specifies to enable tunneling for GARP VLAN Registration Protocol (GVRP) packets.
stp	(Optional) Specifies to enables tunneling for Spanning Tree Protocol (STP) packets.
01-00-0c-cc-cc-cc	(Optional) Specifies to tunnel the protocol packets with this Destination Address (DA).
01-00-0c-cc-cc-cd	(Optional) Specifies to tunnel the protocol packets with this DA.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use the command to enable tunneling of Layer 2 protocol packets. With protocol tunneling, the protocol operation information at the local site and the remote site can be exchanged through the service provider network. If the protocol type is not specified, the command enables tunneling of all types of protocol packets. Configure the Layer 2 protocol tunnel for GVRP/STP on the port whether GVRP/STP is enabled or not. However, the protocol operation of GVRP/STP will not work on the port when the corresponding Layer 2 protocol tunnel for GVRP/STP is enabled.
When a Layer 2 protocol packet arrives at port which is enabled for protocol tunneling, the Switch will classify the packet with the service VLAN and forward the packet to the service VLAN member ports. Generally, the packet is encapsulated and forwarded to the remote site via the trunk port. When forwarding a packet to the remote site via a trunk port, the tunneled packet will be tagged with service VLAN. The packet can also be forwarded to other ports at the local site which are enabled for protocol tunneling.
Normally, protocol tunneling encapsulates the protocol packet by replacing the destination MAC address of the packet with a vendor specific multicast address. However, if the port being forwarded is Layer 2 protocol tunnel enabled, then the destination MAC address of the protocol packet will not be overwritten.
At the remote site, the Switch decapsulates the tunneled packet by restoring the vendor specific multicast address to the original PDU address and forward the packet to the customer network via the ports that are enabled for protocol tunneling.
If the port that is enabled for the Layer 2 protocol tunnel receives an encapsulated packet, then the port will enter the error-disable state.

Example

This example shows how to enable a tunneling protocol for the STP protocol on an interface.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# l2protocol-tunnel stp

 WARNING: STP doesn't run when l2 protocol tunnel is enabled for the port.
GA-MLxxTPoE+(config-if)#
```

4.11.3 l2protocol-tunnel cos

This command is used to specify the CoS value for tunneling of the protocol packets. Use the no form of this command to revert to the default setting.

Syntax

- l2protocol-tunnel cos *COS-VALUE*
- no l2protocol-tunnel cos

Parameters

Parameters	Description
COS-VALUE	Specifies the CoS value. The values are from 0 to 7. 7 is the highest priority.

Default

By default, this value is 5.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

When a Layer 2 protocol packet arrives at a port that is enabled for the Layer 2 protocol tunnel, the Switch encapsulates the packet with a service VLAN tag and rewrites the CoS with the value specified by this command.

Example

This example shows how to specify a CoS value for tunneling of the protocol packets.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# l2protocol-tunnel cos 7
GA-MLxxTPoE+(config)#
```

4.11.4 l2protocol-tunnel drop-threshold

This command is used to specify the threshold in tunneling of the specified Layer 2 protocol packets received by a port before it is dropped. Use the no form of this command to revert to the default setting.

Syntax

- l2protocol-tunnel drop-threshold [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}] *PPS*
- no l2protocol-tunnel drop-threshold [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}]

Parameters

Parameters	Description
gvrp	(Optional) Specifies GVRP packets.
stp	(Optional) Specifies STP packets.
01-00-0c-cc-cc-cc	(Optional) Specifies the protocol packets with this DA.
01-00-0c-cc-cc-cd	(Optional) Specifies the protocol packets with this DA.
PPS	Specifies the threshold in number of packets per second This value must be between 1 and 4096 packets per second.

Default

By default, no threshold is configured.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The tunneling of Layer 2 protocol packets will consume CPU processing power when encapsulating, decapsulating and forwarding packets. Use this command to restrict the CPU processing bandwidth consumption by specifying a threshold in the tunneling of the specified Layer 2 protocol packets received by a port. When the threshold is exceeded, the excessive incoming packets are dropped. If the protocol type is not specified, the setting applies to all protocol types. The l2protocol-tunnel drop-threshold command can be used together with the l2protocol-tunnel shutdown-threshold command to restrict the processing bandwidth. If the shutdown threshold is also configured on the interface, the drop-threshold value must be less than or equal to the shutdown-threshold value.

Example

This example shows how to configure the drop threshold for the STP protocol.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# l2protocol-tunnel drop-threshold stp 2000
GA-MLxxTPoE+(config-if)#
```

4.11.5 l2protocol-tunnel global drop-threshold

This command is used to specify the maximum number of Layer 2 protocol packets that can be processed by the system per second. Use the **no** form of this command to revert to the default setting.

Syntax

- **l2protocol-tunnel global drop-threshold** *PPS*
- **no l2protocol-tunnel global drop-threshold**

Parameters

Parameters	Description
PPS	Specifies the maximum rate of incoming Layer 2 protocol packets that can be tunneled. This value must be between 100 and 20000.

Default

By default, no threshold is configured.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The tunneling of the Layer 2 protocol packets will consume CPU processing power in encapsulating, decapsulating, and forwarding of the packet. Use the command to restrict the CPU processing bandwidth consumed by specifying a threshold on the number of all Layer 2 protocol packets that can be processed by the system. When the maximum number of packets is exceeded, the excessive protocol packets are dropped.
Use the **l2protocol-tunnel global drop-threshold** command and the **l2protocol-tunnel drop-threshold** command in the global configuration mode to leverage the bandwidth restriction.

Example

This example shows how to enable rate limiting globally.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# l2protocol-tunnel global drop-threshold 5000
GA-MLxxTPoE+(config)#
```

4.11.6 l2protocol-tunnel shutdown-threshold

This command is used to specify a threshold in the tunneling of the specified Layer 2 protocol packets received by a port before the shutdown. Use the **no** form of this command to revert to the default setting.

Syntax

- **l2protocol-tunnel shutdown-threshold [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}]** *PPS*
- **no l2protocol-tunnel shutdown-threshold [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}]**

Parameters

Parameters	Description
gvrp	(Optional) Specifies GVRP tunneling.
stp	(Optional) Specifies STP tunneling.
01-00-0c-cc-cc-cc	(Optional) Specifies the protocol packets with this DA.
01-00-0c-cc-cc-cd	(Optional) Specifies the protocol packets with this DA.
PPS	Specifies the threshold in number of packets per second This value must be between 1 and 4096 packets.

Default

By default, no threshold is configured.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use the command to restrict the CPU processing bandwidth consumption by specifying a threshold for tunneling of the specified Layer 2 protocol packets received the port. When the threshold is exceeded, the port is put in error-disabled state.
If protocol type is not specified, the setting applies to all protocol types.
The **l2protocol-tunnel shutdown-threshold** command can be used together with the **l2protocol-tunnel drop-threshold** command. If drop threshold is also configured on the interface, the shutdown-threshold value must be greater than or equal to the drop-threshold value.

Example

This example shows how to specify the maximum number of STP packets that can be processed on that interface in 1 second.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# l2protocol-tunnel shutdown-threshold stp 200
GA-MLxxTPoE+(config-if)#
```

4.11.7 l2protocol-tunnel mac-address

This command is used to specify the L2PT tunneling multicast address for the specified protocol. Use the **no** form of this command to revert to the default setting.

Syntax

- **l2protocol-tunnel mac-address [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}]** *MAC-ADDR*

- no l2protocol-tunnel mac-address [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}]

Parameters

Parameters	Description
gvrp	(Optional) Specifies the GVRP packets to be tunneled to the specified address.
stp	(Optional) Specifies the STP packets to be tunneled to the specified address.
01-00-0c-cc-cc-cc	(Optional) Specifies the protocol packets with this DA to be tunneled to the specified address.
01-00-0c-cc-cc-cd	(Optional) Specifies the protocol packets with this DA to be tunneled to the specified address.
MAC-ADDR	Specifies MAC address for the packets to be tunneled to. The address should not be reserved or used by other protocols.

Default

By default, the tunneling address of GVRP is 00-C0-8F-04-92-C1.
By default, the tunneling address of STP is 00-C0-8F-04-92-C0.
By default, the tunneling address of protocol MAC 01-00-0C-CC-CC-CC is 00-C0-8F-04-92-C2.
By default, the tunneling address of protocol MAC 01-00-0C-CC-CC-CD is 00-C0-8F-04-92-C3.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use the command to specify the L2PT tunneling multicast address for the specified protocol.
If protocol type is not specified, the setting applies to all protocol types.
The following MAC addresses are reserved or used by other protocols, and should not be configured in the command:

- FF-FF-FF-FF-FF-FF
- 00-00-00-00-00-00

- 01-00-0C-CC-CC-CC
- 01-00-0C-CC-CC-CD
- 01-80-C2-00-00-00 to 01-80-C2-00-00-0F
- 01-80-C2-00-00-10
- 01-80-C2-00-00-20 to 01-80-C2-00-00-2F
- 01-00-5E-00-00-00 to 01-00-5E-FF-FF-FF
- 33-33-00-00-00-04
- 33-33-00-00-00-05
- 33-33-00-00-00-06
- 33-33-00-00-00-09
- 33-33-00-00-00-0D
- 00-C0-8F-04-93-00
- 00-C0-8F-00-00-02

Example

This example shows how to specify the L2PT tunneling multicast address of STP to 01-00-0c-cd-cd-d0.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#l2protocol-tunnel mac-address stp 01-00-0c-cd-cd-d0
GA-MLxxTPoE+(config)#
```

4.11.8 show l2protocol-tunnel

This command is used to display the protocols that are tunneled on an interface or on all interfaces.

Syntax

- **show l2protocol-tunnel [interface** *INTERFACE-ID*]

Parameters

Parameters	Description
interface *INTERFACE-ID*	(Optional) Specifies the interface to display.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display the Layer 2 protocol tunnel related settings, status, and counters.

Example

This example shows how to display the protocols that are tunneled on all interfaces.

```
GA-MLxxTPoE+#show l2protocol-tunnel

CoS for Encapsulated Packets            :5
Drop Threshold for Encapsulated Packets :0

Protocol             Drop Counter    Tunneling Address
-----------------    ------------    -----------------
gvrp                 0               00-C0-8F-04-92-C1
stp                  0               00-C0-8F-04-92-C0
01-00-0c-cc-cc-cc    0               00-C0-8F-04-92-C2
01-00-0c-cc-cc-cd    0               00-C0-8F-04-92-C3

Port       Protocol     Shutdown  Drop      Encap      Decap      Drop
                        Threshold Threshold Counter    Counter    Counter
---------- ------------ --------- --------- ---------- ---------- ----------
Gi1/0/3    gvrp         -         2000      8          0          0
Gi1/0/5    gvrp         -         2000      8          0          0
           stp          -         2000      1268       1100       0
           01000ccccccc -         2000      0          0          0

GA-MLxxTPoE+#
```

Display Parameters

Parameters	Description
CoS for Encapsulated Packets	Indicates the Class of Service (CoS) value for tunneled L2 protocol packets.
Drop Threshold for Encapsulated Packets	Indicates the rate limiting on L2PT.
Protocol	Indicates the type of L2 protocol to be tunneled.
Drop Counter	Indicates the number of specified L2 protocol packets which are dropped.
Tunneling Address	Indicates the protocol tunneling multicast address setting.
Port	Indicates the port that is enabled for L2PT.
Shutdown Threshold	Indicates the shutdown threshold for specified L2 protocol packet.

Parameters	Description
Drop Threshold	Indicates the drop threshold for the specified L2 protocol packet.
Encap Counter	Indicates the number of L2 protocol packets received and encapsulated by the L2PT-enabled port.
Decap Counter	Indicates the number of L2 protocol packets decapsulated and transmitted to the L2PT-enabled port.

4.12 Line Loopback Commands

4.12.1 line loopback enable (Global)

This command is used to enable the line loopback function globally. Use the **no** form of this command to disable the function globally.

Syntax

line loopback enable

no line loopback enable

Parameters

None

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode

Command Default Level

Level：12

Usage Guideline

This command is used to enable the line loopback function globally.

Example

This example shows how to enable line loopback function globally.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# line loopback enable
GA-MLxxTPoE+(config)#
```

4.12.2 line loopback (Interface)

This command is used to enable the line loopback function for an interface. Use the no form of this command to disable the function for an interface.

Syntax

line loopback

no line loopback

Parameters

None

Default

By default, this option is enabled on Gigabit Ethernet ports and disabled on other ports.

Command Mode

Interface Configuration Mode

Command Default Level

Level：12

Usage Guideline

Use this command to enable the line loopback function on an interface. This command is available for physical port and port-channel interface configuration.

Example

This example shows how to enable the line loopback function on interface Gigabit Ethernet port 1/0/1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#line loopback
GA-MLxxTPoE+(config-if)#
```

4.12.3 line loopback mode

This command is used to line loopback mode. Use the **no** form of this command to revert to the default setting.

Syntax

line loopback mode {block | shutdown}

Parameters

Parameters	概要
block	Specifies that the port enters the block mode when detecting loop.
shutdown	Specifies that the port first enters the shutdown mode and then the block mode when detecting loop.

Default

By default, the mode is block.

Command Mode

Interface Configuration Mode

Command Default Level

Level：12

Usage Guideline

In the **block** mode, when a loop is detected on a port, the Switch will generate Loop Detection Frames and probe the port until the loop is resolved. After the port receives a Loop Detection Frame, it will enter the **Blocking** state. During the **line loopback recovery** time, the port will enter the **Forwarding** state if no Loop Detection Frame was received by the port.

In the **shutdown** mode, when a loop is detected on a port, the Switch will generate Loop Detection Frames and probe the port until the loop is resolved. After the port receives a Loop Detection Frame, it will immediately enter the **Shutdown** state first and then change to the **Blocking** state. At the start of the last 30 seconds of the **line loopback recovery** time, the port will return to the **Up**

state. During the last 30 seconds of the **line loopback recovery** time, the port will enter the **Forwarding** state if no Loop Detection Frame was received by the port.

Example

This example shows how to configure the line loopback mode to the shutdown mode for Gigabit Ethernet port 1/0/1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#line loopback mode shutdown
GA-MLxxTPoE+(config-if)#
```

4.12.4 line loopback recovery

This command is used to configure the auto-recovery time for line loopback. Use the **no** form of this command to disable auto-recovery.

Syntax

- **line loopback recovery** *SECONDS*

  no line loopback recovery

Parameters

Parameters	概要
SECONDS	Specifies the auto-recovery time in seconds. The valid range is from 60 to 86400 (seconds).

Default

By default, the auto-recovery time is 60 seconds.

Command Mode

Interface Configuration Mode

Command Default Level

Level：12

Usage Guideline

Use this command to configure the auto-recovery time for line loopback. When this is enabled and the loop is detected, the port state will return to normal after the auto-recovery time expires.

Example

This example shows how to configure the auto-recovery time to 100 seconds for Gigabit Ethernet port 1/0/1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#line loopback recovery 100
GA-MLxxTPoE+(config-if)#
```

4.12.5 show line loopback configuration

This command is used to display the current line loopback control settings.

Syntax

show line loopback configuration

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level：1

Usage Guideline

Use this command to display the line loopback setting and status.

Example

This example shows how to display the current line loopback settings and status.

```
GA-MLxxTPoE+#show line loopback configuration

 Global Loop Detection Status : Enabled
 Interface      Link     State      Loop Detect    Mode     Recovery  RecoveryTime
 -------------  ----  -----------  -----------  --------  --------  ------------
 Gi1/0/1        Up    Forwarding   Enabled      Shutdown  Enabled        100
 Gi1/0/2        Down  Forwarding   Enabled      Block     Enabled         60
 Gi1/0/3        Up    Forwarding   Enabled      Block     Enabled         60
 Gi1/0/4        Down  Forwarding   Enabled      Block     Enabled         60
 Gi1/0/5        Down  Forwarding   Enabled      Block     Enabled         60
 Gi1/0/6        Down  Forwarding   Enabled      Block     Enabled         60
 Gi1/0/7        Down  Forwarding   Enabled      Block     Enabled         60
 Gi1/0/8        Down  Forwarding   Enabled      Block     Enabled         60
 Gi1/0/9        Down  Forwarding   Enabled      Block     Enabled         60
 Gi1/0/10       Down  Forwarding   Enabled      Block     Enabled         60
 Gi1/0/11       Down  Forwarding   Enabled      Block     Enabled         60
 Gi1/0/12       Down  Forwarding   Enabled      Block     Enabled         60
 Gi1/0/13       Down  Forwarding   Enabled      Block     Enabled         60
 Gi1/0/14       Down  Forwarding   Enabled      Block     Enabled         60
 Gi1/0/15       Down  Forwarding   Enabled      Block     Enabled         60
 Gi1/0/16       Down  Forwarding   Enabled      Block     Enabled         60
 Gi1/0/17       Down  Forwarding   Enabled      Block     Enabled         60
 Gi1/0/18       Down  Forwarding   Enabled      Block     Enabled         60
 Gi1/0/19       Down  Forwarding   Enabled      Block     Enabled         60
 Gi1/0/20       Down  Forwarding   Enabled      Block     Enabled         60
--More--
```

Display Parameters

Parameters	Description
Interface	Indicates the port that has line loopback enabled.
Link	Indicates the link state of the port.
State	Indicates the port state.
Loop Detect	Indicates the line loop state.
Mode	Indicates the line loop mode.
Recovery	Indicates the auto-recovery state.
Recovery Time	Indicates the auto-recovery time.

4.12.6 show line loopback history

This command is used to display the line loopback history.

Syntax

show line loopback history

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level：1

Usage Guideline

Use this command to display the line loopback history. This is saved in DRAM and can be saved to flash by using the **logging buffered [write-delay {***SECONDS* **| infinite}]** command. When a loop is detected, the Switch records the looping message to syslog and loop history, and sends the SNMP private trap.

Example

This example shows how to display the line loopback history.

```
GA-MLxxTPoE+#show line loopback history

 Entry  Time(YYYY/MM/DD HH:MM:SS)        Event
 -----  ------------------------ ----------------------------------------------
    1    2017/06/28 20:13:07      The loop detected between port Gi1/0/9 and Gi1
                                  /0/10.
    2    2017/06/28 20:13:55      The loop detected between port Gi1/0/15 and Gi
                                  1/0/16.

GA-MLxxTPoE+#
```

4.12.7 clear line loopback history

This command is used to clear the line loopback history saved in DRAM.

Syntax

clear line loopback histroy

Parameters

None

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level：12

Usage Guideline

Use this command to clear the line loopback history saved in DRAM.

Example

This example shows how to clear the line loopback history saved in DRAM.

```
GA-MLxxTPoE+#clear line loopback history

GA-MLxxTPoE+#
```

4.12.8 snmp-server enable traps line loopback

This command is used to enable the sending of SNMP notifications for line loopback. Use the no form of this command to revert to the default setting.

Syntax

snmp-server enable traps line loopback

no snmp-server enable traps line loopback

Parameters

None

Default

By default, this feature is disabled

Command Mode

Global Configuration Mode

Command Default Level

Level：12

Usage Guideline

This command is used to enable or disable the sending of SNMP notifications for line loopback.

Example

This example shows how to enable the sending of SNMP notifications for line loopback.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#snmp-server enable traps line loopback
GA-MLxxTPoE+(config)#
```

5 Traffic Control

5.1 Access Control List (ACL) Commands

For network security protection, blocking unauthorized access from internal and external sources is important.
Access Control is a function to filter packet transfer by setting rules after checking the header information of packets that reach the switch. To use the Access Control function, you need to create an Access Control List (ACL), which defines filtering targets, conditions, and actions, and configure target ports and VLANs.

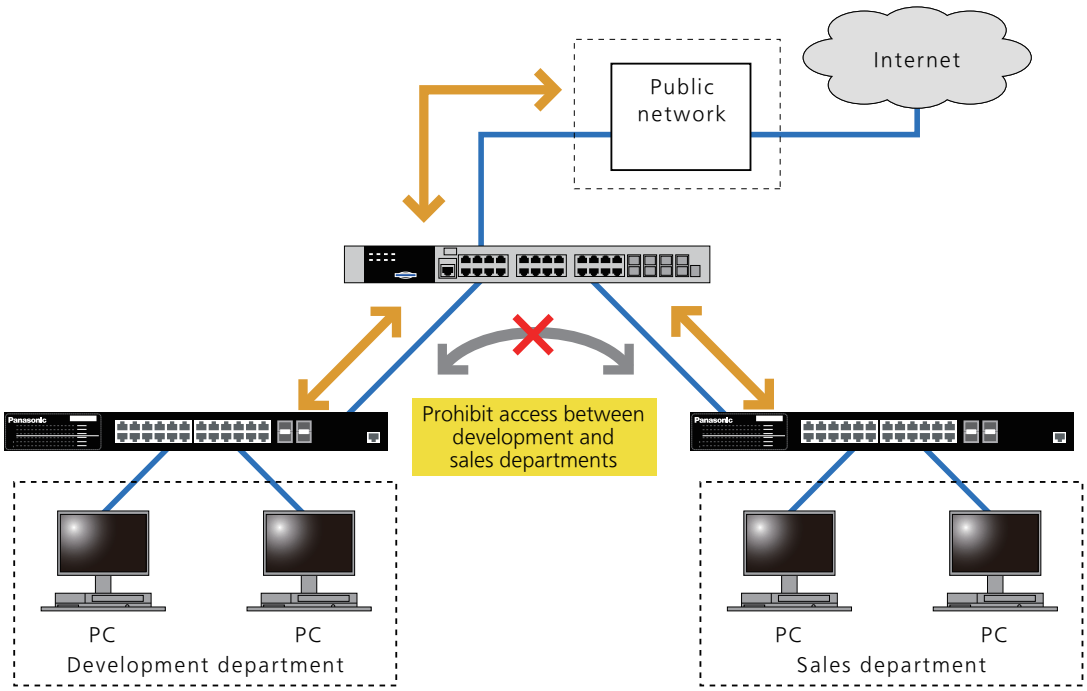


Figure 40-1 Access Control overview

5.1.1 access-list resequence

This command is used to re-sequence the starting sequence number and the increment number of the access list entries in an access list. Use the **no** form of this command to revert to the default setting.

Syntax

- **access-list resequence** {*NAME* | *NUMBER*} *STARTING-SEQUENCE-NUMBER INCREMENT*

- no access-list resequence

Parameters

Parameters	Description
NAME	Specifies the name of the access list to be configured. It can be a maximum of 32 characters.
NUMBER	Specifies the number of the access list to be configured.
STARTING-SEQUENCE-NUMBER	Specifies that the access list entries will be re-sequenced using this initial value. The range of possible sequence numbers is 1 through 65535.
INCREMENT	Specifies the number that the sequence numbers step. The default value is 10. For example, if the increment (step) value is 5 and the beginning sequence number is 20, the subsequent sequence numbers are 25, 30, 35, 40, and so on. The range of valid values is from 1 to 32.

Default

The default start sequence number is 10.
The default increment is 10.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This feature allows the user to re-sequence the entries of a specified access list with an initial sequence number determined by the *STARTING-SEQUENCE-NUMBER* parameter and continuing in the increments determined by the *INCREMENT* parameter. If the highest sequence number exceeds the maximum possible sequence number, then there will be no re-sequencing.
If a rule entry is created without specifying the sequence number, the sequence number will be automatically assigned. If it is the first entry, a start sequence number is assigned. Subsequent rule entries are assigned a sequence number that is an increment value greater than the largest sequence number in that access list and the entry is placed at the end of the list.

After the start sequence number or increment change, the sequence number of all previous rules (include the rules that assigned sequence by user) will change according to the new sequence setting.

Example

This example shows how to re-sequence the sequence number of an IP access-list, named R&D.

```
GA-MLxxTPoE+# show access-list ip R&D

Extended IP access list R&D(ID: 3999)
     10 permit tcp any 10.20.0.0 0.0.255.255
     20 permit tcp any host 10.100.1.2
     30 permit icmp any any

GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#ip access-list extended R&D
GA-MLxxTPoE+(config-ip-ext-acl)# 5 permit tcp any 10.30.0.0 0.0.255.255
GA-MLxxTPoE+(config-ip-ext-acl)# end
GA-MLxxTPoE+# show access-list ip R&D

Extended IP access list R&D(ID: 3999)
     5 permit tcp any 10.30.0.0 0.0.255.255
     10 permit tcp any 10.20.0.0 0.0.255.255
     20 permit tcp any host 10.100.1.2
     30 permit icmp any any

GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)# access-list resequence R&D 1 2
GA-MLxxTPoE+(config)# end
GA-MLxxTPoE+# show access-list ip R&D

     Extended IP access list R&D(ID: 3999)
     1 permit tcp any 10.30.0.0 0.0.255.255
     3 permit tcp any 10.20.0.0 0.0.255.255
     5 permit tcp any host 10.100.1.2
     7 permit icmp any any

GA-MLxxTPoE+#
```

5.1.2 acl-hardware-counter

This command is used to enable the ACL hardware counter of the specified access-list name for access group functions or access map for the VLAN filter function. Use the **no** form of this command to disable the ACL hardware counter function.

Syntax

- **acl-hardware-counter** {**access-group** {*ACCESS-LIST-NAME* | *ACCESS-LIST-NUMBER*} | **vlan-filter** *ACCESS-MAP-NAME*}

- **no acl-hardware-counter** {**access-group** {*ACCESS-LIST-NAME* | *ACCESS-LIST-NUMBER*} | **vlan-filter** *ACCESS-MAP-NAME*}

Parameters

Parameters	Description
access-group *ACCESS-LIST-NAME*	Specifies the name of the access list to be configured.
access-group *ACCESS-LIST-NUMBER*	Specifies the number of the access list to be configured.
vlan-filter *ACCESS-MAP-NAME*	Specifies the name of the access map to be configured.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command with parameter **access-group** will enable the ACL hardware counter for all ports that have applied the specified access-list name or number. The number of packets that match each rule are counted.
The command with parameter **vlan-filter** will enable the ACL hardware counter for all VLAN(s) that have applied the specified VLAN access-map. The number of packets permitted by each access map are counted.

Example

This example shows how to enable the ACL hardware counter.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# acl-hardware-counter access-group abc
GA-MLxxTPoE+(config)#
```

5.1.3 action

This command is used to configure the forward, drop, or redirect action of the sub-map in the VLAN access-map sub-map configuration mode. Use the **no** form of this command to revert to the default setting.

Syntax

- **action** {**forward** | **drop** | **redirect** *INTERFACE-ID*}
- **no action**

Parameters

Parameters	Description
forward	Specifies to forward the packet when matched.
drop	Specifies to drop the packet when matched.
redirect *INTERFACE-ID*	Specifies the interface ID for the redirection action. Only physical ports are allowed to be specified.

Default

By default, the action is **forward**.

Command Mode

VLAN Access-map Sub-map Configuration Mode.

Command Default Level

Level: 12

Usage Guideline

One sub-map has only one action. The action configured later overwrites the previous action. A VLAN access map can contain multiple sub-maps. The packet that matches a sub-map (a packet permitted by the associated access-list) will take the action specified for the sub-map. No further checking against the next sub-maps is done. If the packet does not match a sub-map, then the next sub-map will be checked.

Example

This example shows how to configure the action in the sub-map.

```
GA-MLxxTPoE+# show vlan access-map
VLAN access-map vlan-map 20
  match mac access list: ext_mac(ID: 7999)
  action: forward
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan access-map vlan-map 20
GA-MLxxTPoE+(config-access-map)# action redirect gi1/0/5
GA-MLxxTPoE+(config-access-map)# end
GA-MLxxTPoE+# show vlan access-map
VLAN access-map vlan-map 20
  match mac access list:  ext_mac(ID: 7999)
  action: redirect Gi1/0/5
GA-MLxxTPoE+#
```

5.1.4 clear acl-hardware-counter

This command is used to clear the ACL hardware counter.

Syntax

- **clear acl-hardware-counter** {**access-group** [*ACCESS-LIST-NAME* | *ACCESS-LIST-NUMBER*] | **vlan-filter** [*ACCESS-MAP-NAME*]}

Parameters

Parameters	Description
access-group	Specifies to clear the access group.
ACCESS-LIST-NAME	(Optional) Specifies the name of the access list to be cleared.
ACCESS-LIST-NUMBER	(Optional) Specifies the number of the access list to be configured.
vlan-filter	Specifies to clear VLAN filter.
ACCESS-MAP-NAME	(Optional) Specifies the name of the access map to be cleared.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

If no access-list name or number is specified with the parameter **access-group**, all access-group hardware counters will be cleared. If no access-map name is specified with the parameter **vlan-filter**, all VLAN filter hardware counters will be cleared.

Example

This example shows how to clear the ACL hardware counter.

```
GA-MLxxTPoE+#clear acl-hardware-counter access-group abc
GA-MLxxTPoE+#
```

5.1.5 expert access-group

This command is used to apply a specific expert ACL to an interface. Use the **no** form of this command to cancel the application.

Syntax

- **expert access-group** {*NAME* | *NUMBER*} [**in** | **out**]
- **no expert access-group** [*NAME* | *NUMBER*] [**in** | **out**]

Parameters

Parameters	Description
NAME	Specifies the name of the expert access-list to be configured. The name can be up to 32 characters.
NUMBER	Specifies the number of the expert access list to be configured.
in	(Optional) Specifies to filter the incoming packets of the interface. If the direction is not specified, **in** is used.
out	(Optional) Specifies to filter the outgoing packets to transmit to the interface.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for physical port interface configuration.

If expert access group is already configured on the interface, the command applied later will overwrite the previous setting. Only one access-list of the same type can be applied to the same interface; but access-lists of different types can be applied to the same interface.

If the access-list is assigned to the egress interface, rules that are for this access-list and with the TCP/UDP port range field will be ignored.

Example

This example shows how to apply an expert ACL to an interface. The purpose is to apply the ACL **exp_acl** on the GigabitEthernet1/0/2 to filter the incoming packets.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/2
GA-MLxxTPoE+(config-if)# expert access-group exp_acl in

 PROMPT: The remaining applicable EXPERT related access entries are 1920
GA-MLxxTPoE+(config-if)#
```

5.1.6 expert access-list

This command is used to create or modify an extended expert ACL. This command will enter into the extended expert access-list configuration mode Use the **no** form of this command to remove an extended expert access-list.

Syntax

- **expert access-list extended** *NAME* [*NUMBER*]
- **no expert access-list extended** {*NAME* | *NUMBER*}

Parameters

Parameters	Description
NAME	Specifies the name of the extended expert access list to be configured. The name can be up to 32 characters.
NUMBER	Specifies the ID number of expert access list. For extended expert access lists, the value is from 8000 to 9999.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The name must be unique among all access lists. The characters used in the name are case sensitive. If the access list number is not specified, the biggest unused number in the range of the expert access list numbers will be assigned automatically.

Example

This example shows how to create an extended expert ACL.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#expert access-list extended exp_acl
GA-MLxxTPoE+(config-exp-nacl)#
```

5.1.7 ip access-group

This command is used to specify the IP access list to be applied to an interface. Use the **no** form of this command to remove an IP access list.

Syntax

- **ip access-group** {*NAME* | *NUMBER*} [**in** | **out**]
- **no ip access-group** [*NAME* | *NUMBER*] [**in** | **out**]

Parameters

Parameters	Description
NAME	Specifies the name of the IP access list to be applied. The maximum length is 32 characters.
NUMBER	Specifies the number of the IP access list to be applied.
in	(Optional) Specifies that the IP access list will be applied to check packets in the ingress direction. If the direction is not specified, **in** is used.
out	(Optional) Specifies that the IP access list will be applied to check packets in the egress direction.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for physical port interface configuration.

If an IP access group is already configured on the interface, the command applied later will overwrite the previous setting. Only one access list of the same type can be applied to the same interface; but access lists of different types can be applied to the same interface.
The association of an access group with an interface will consume the filtering entry resource in the Switch controller. If the resources are insufficient to commit the command, then an error message will be displayed. There is a limitation on the number of port operator resources. If applying the command exhausts the available port selectors, then an error message will be displayed.

There is a limitation on the number of port operator resources. If applying the command exhausts the available port selectors, an error message will be displayed.

Example

This example shows how to specify the IP access list “Strict-Control” as an IP access group for GigabitEthernet1/0/2.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/2
GA-MLxxTPoE+(config-if)#ip access-group Strict-Control in

 PROMPT: The remaining applicable IP related access entries are 3840, remaining range
entries are 32.
GA-MLxxTPoE+(config-if)#
```

5.1.8 ip access-list

This command is used to create or modify an IP access list. This command will enter into the IP access list configuration mode. Use the **no** form of this command to remove an IP access list.

Syntax

- **ip access-list** [**extended**] *NAME* [*NUMBER*]
- **no ip access-list** [**extended**] {*NAME* | *NUMBER*}

Parameters

Parameters	Description
extended	(Optional) Specifies that the IP access list is the extended IP access list, and more fields can be chosen for the filter. If the parameter is not specified, the IP access list is the standard IP access list.
NAME	Specifies the name of the IP access list to be configured. The maximum length is 32 characters. The first character must be a letter.
NUMBER	Specifies the ID number of the IP access list. For standard IP access lists, this value is from 1 to 1999. For extended IP access lists, this value is from 2000 to 3999.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The name must be unique among all access lists. The characters used in the name are case sensitive. If the access list number is not specified, the biggest unused number in the range of IP access list numbers will be assigned automatically.

Example

This example shows how to configure an extended IP access list, named "Strict-Control" and an IP access-list, named "pim-srcfilter".

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip access-list extended Strict-Control
GA-MLxxTPoE+(config-ip-ext-acl)# permit tcp any 10.20.0.0 0.0.255.255
GA-MLxxTPoE+(config-ip-ext-acl)# exit
GA-MLxxTPoE+(config)# ip access-list pim-srcfilter
GA-MLxxTPoE+(config-ip-acl)# permit host 172.16.65.193 any
GA-MLxxTPoE+(config-ip-acl)#
```

5.1.9 ipv6 access-group

This command is used to specify the IPv6 access list to be applied to an interface. Use the **no** form of this command to remove an IPv6 access list.

Syntax

- **ipv6 access-group** {*NAME* | *NUMBER*} [**in** | **out**]
- **no ipv6 access-group** [*NAME* | *NUMBER*] [**in** | **out**]

Parameters

Parameters	Description
NAME	Specifies the name of the IPv6 access list to be applied.
NUMBER	Specifies the number of the IPv6 access list to be applied.
in	(Optional) Specifies that the IPv6 access list will be applied to check in the ingress direction. If the direction is not specified, **in** is used.
out	(Optional) Specifies that the IPv6 access list will be applied to check in the egress direction.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for physical port interface configuration.
Only one access list of the same type can be applied to the same interface, but access lists of different types can be applied to the same interface. The association of an access group with an interface will consume the filtering entry resource in the switch controller. If the resource is insufficient to commit the command, then an error message will be displayed.
There is a limitation on the number of port operator resources. If applying the command exhausts the available port selectors, an error message will be displayed.

Example

This example shows how to specify the IPv6 access list “ip6-control” as an IP access group for GigabitEthernet1/0/3.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/3
GA-MLxxTPoE+(config-if)#ipv6 access-group ip6-control

 PROMPT: The remaining applicable IPv6 related access entries are 896
GA-MLxxTPoE+(config-if)#
```

5.1.10 ipv6 access-list

This command is used to create or modify an IPv6 access list. This command will enter into IPv6 access-list configuration mode. Use the **no** form of this command to remove an IPv6 access list.

Syntax

- **ipv6 access-list [extended]** *NAME* [*NUMBER*]
- **no ipv6 access-list [extended]** {*NAME* | *NUMBER*}

Parameters

Parameters	Description
extended	(Optional) Specifies that the IPv6 access list is the extended IPv6 access list, and more fields can be chosen for the filter. If the parameter is not specified, the IPv6 access list is the standard IPv6 access list.
NAME	Specifies the name of the IPv6 access list to be configured. The maximum length is 32 characters.
NUMBER	Specifies the ID number of the IPv6 access list. For standard IPv6 access lists, this value is from 11000 to 12999. For extended IPv6 access lists, this value is from 13000 to 14999.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The name must be unique among all access lists. The characters used in the name are case sensitive. If the access list number is not specified, the biggest unused number in the range of the IPv6 access list numbers will be assigned automatically.

Example

This example shows how to configure an IPv6 extended access list, named ip6-control.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ipv6 access-list extended ip6-control
GA-MLxxTPoE+(config-ipv6-ext-acl)# permit tcp any 2002:f03::1/16
GA-MLxxTPoE+(config-ipv6-ext-acl)#
```

This example shows how to configure an IPv6 standard access list, named ip6-std-control.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ipv6 access-list ip6-std-control
GA-MLxxTPoE+(config-ipv6-acl)# permit any fe80::101:1/54
GA-MLxxTPoE+(config-ipv6-acl)#
```

5.1.11 list-remark

This command is used to add remarks for the specified ACL. Use the **no** form of this command to delete the remarks.

Syntax

- **list-remark** *TEXT*
- **no list-remark**

Parameters

Parameters	Description
TEXT	Specifies the remark information. The information can be up to 256 characters long.

Default

None

Command Mode

Access-list Configuration Mode.

Command Default Level

Level: 12

Usage Guideline

This command is available in the MAC, IP, IPv6, and Expert Access-list Configure mode.

Example

This example shows how to add a remark to the access-list.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)#ip access-list extended R&D
GA-MLxxTPoE+(config-ip-ext-acl)# list-remark This access-list is used to match any IP
packets from the host 10.2.2.1.
GA-MLxxTPoE+(config-ip-ext-acl)# end
GA-MLxxTPoE+# show access-list ip

Extended IP access list R&D(ID: 3999)
  10 permit host 10.2.2.1 any
  This access-list is used to match any IP packets from the host 10.2.2.1.

GA-MLxxTPoE+#
```

5.1.12 mac access-group

This command is used to specify a MAC access list to be applied to an interface. Use the **no** form of this command to remove the access group control from the interface.

Syntax

- **mac access-group** {*NAME* | *NUMBER*} [**in** | **out**]
- **no mac access-group** [*NAME* | *NUMBER*] [**in** | **out**]

Parameters

Parameters	Description
NAME	Specifies the name of the MAC access list to be applied.
NUMBER	Specifies the number of the MAC access list to be applied.
in	(Optional) Specifies that the MAC access list will be applied to check in the ingress direction. If direction is not specified, **in** is used.
out	(Optional) Specifies that the MAC access list will be applied to check in the egress direction.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for physical port interface configuration.
If MAC access group is already configured on the interface, the command applied later will overwrite the previous setting. MAC access-groups will only check non-IP packets.
Only one access list of the same type can be applied to the same interface, but access lists of different types can be applied to the same interface.
The association of an access group with an interface will consume the filtering entry resource in the switch controller. If the resource is insufficient to commit the command, then an error message will be displayed.

Example

This example shows how to apply the MAC access list daily-profile to GigabitEthernet1/0/4.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/4
GA-MLxxTPoE+(config-if)#mac access-group daily-profile in

 PROMPT: The remaining applicable MAC related access entries are 1280.
GA-MLxxTPoE+(config-if)#
```

5.1.13 mac access-list

This command is used to create or modify an MAC access list and this command will enter the MAC access list configuration mode. Use the **no** form of this command to delete a MAC access list.

Syntax

- **mac access-list extended** *NAME* [*NUMBER*]
- **no mac access-list extended** {*NAME* | *NUMBER*}

Parameters

Parameters	Description
NAME	Specifies the name of the MAC access list to be configured. The maximum length is 32 characters.
NUMBER	Specifies the ID number of the MAC access list. For extended MAC access lists, this value is from 6000 to 7999.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to enter the MAC Access-list Configuration mode, and use the **permit** or **deny** command to specify the entries. The name must be unique among all access lists. The characters of the name are case sensitive. If the access list number is not specified, the biggest unused number in the range of the MAC access list numbers will be assigned automatically.

Example

This example shows how to enter the MAC access list configuration mode for a MAC access list named “daily profile”.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# mac access-list extended daily-profile
GA-MLxxTPoE+(config-mac-ext-acl)#
```

5.1.14 match ip address

This command is used to associate an IP access list for the configured sub-map. Use the **no** form of this command to remove the matched entry.

Syntax

- **match ip address** {*ACL-NAME* | *ACL-NUMBER*}
- **no match ip address**

Parameters

Parameters	Description
ACL-NAME	Specifies the name of the ACL access list to be configured. The name can be up to 32 characters.

Parameters	Description
ACL-NUMBER	Specifies the number of the IP ACL access list to be configured.

Default

None

Command Mode

VLAN Access-map Sub-map Configuration Mode.

Command Default Level

Level: 12

Usage Guideline

Use this command to associate an IP access list with the configured sub-map. One sub-map can only be associated with one access list (IP access list, IPv6 access list, or MAC access list). The IP sub-map only checks IP packets. Newer commands will overwrite the previous settings.

Example

This example shows how to configure the match content in the sub-map.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan access-map vlan-map 20
GA-MLxxTPoE+(config-access-map)# match ip address sp1
GA-MLxxTPoE+(config-access-map)#
```

5.1.15 match ipv6 address

This command is used to associate IPv6 access lists for the configured sub-maps. Use the **no** form of this command to remove the matched entry.

Syntax

- **match ipv6 address** {*ACL-NAME* | *ACL-NUMBER*}
- **no match ipv6 address**

Parameters

Parameters	Description
ACL-NAME	Specifies the name of the IPv6 ACL access list to be configured. The name can be up to 32 characters.
ACL-NUMBER	Specifies the number of the IPv6 ACL access list to be configured.

Default

None

Command Mode

VLAN Access-map Sub-map Configuration Mode.

Command Default Level

Level: 12

Usage Guideline

Use this command to associate an IPv6 access list with the configured sub-map. One sub-map can only be associated with one access list (IP access list, IPv6 access list, or MAC access list). The IPv6 sub-map only checks IPv6 packets. Newer commands will overwrite the previous settings.

Example

This example shows how to set the match content in the sub-map.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan access-map vlan-map 20
GA-MLxxTPoE+(config-access-map)# match ipv6 address sp1
GA-MLxxTPoE+(config-access-map)#
```

5.1.16 match mac address

This command is used to associate MAC access lists for the configured sub-maps. Use the **no** form of this command to remove the matched entry.

Syntax

- **match mac address** {*ACL-NAME* | *ACL-NUMBER*}
- **no match mac address**

Parameters

Parameters	Description
ACL-NAME	Specifies the name of the ACL MAC access list to be configured. The name can be up to 32 characters.
ACL-NUMBER	Specifies the number of the ACL MAC access list to be configured.

Default

None

Command Mode

VLAN Access-map Sub-map Configuration Mode.

Command Default Level

Level: 12

Usage Guideline

Use this command to associate a MAC access list with the configured sub-map. One sub-map can only be associated with one access list (IP access list, IPv6 access list, or MAC access list). The MAC sub-map only checks non-IP packets. Newer commands will overwrite the previous settings.

Example

This example shows how to set the match content in the sub-map.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan access-map vlan-map 30
GA-MLxxTPoE+(config-access-map)# match mac address ext_mac
GA-MLxxTPoE+(config-access-map)#
```

5.1.17 permit | deny (expert access-list)

This command is used to add a permit or deny entry. Use the **no** form of this command to remove an entry.

Syntax

Extended Expert ACL:

[*SEQUENCE-NUMBER*] {permit | deny} *PROTOCOL* {*SRC-IP-ADDR SRC-IP-WILDCARD* | host *SRC-IP-ADDR* | any} {*SRC-MAC-ADDR SRC-MAC-WILDCARD* | host *SRC-MAC-ADDR* | any} {*DST-IP-ADDR DST-IP-WILDCARD* | host *DST-IP-ADDR* | any} {*DST-MAC-ADDR DST-MAC-WILDCARD* | host *DST-MAC-ADDR* | any} [cos *OUTER-COS* [*MASK*] [vlan *OUTER-VLAN* [*MASK*] [fragments] [[precedence *PRECEDENCE* [*MASK*]] [tos *TOS* [*MASK*]] | dscp *DSCP* [*MASK*]] [time-range *PROFILE-NAME*]

[*SEQUENCE-NUMBER*] {permit | deny} tcp {*SRC-IP-ADDR SRC-IP-WILDCARD* | host *SRC-IP-ADDR* | any} {*SRC-MAC-ADDR SRC-MAC-WILDCARD* | host *SRC-MAC-ADDR* | any} [{eq | lt | gt | neq} *PORT* | range *MIN-PORT MAX-PORT* | mask *PORT MASK*] {*DST-IP-ADDR DST-IP-WILDCARD* | host *DST-IP-ADDR* | any} {*DST-MAC-ADDR DST-MAC-WILDCARD* | host *DST-MAC-ADDR* | any} [{eq | lt | gt | neq} *PORT* | range *MIN-PORT MAX-PORT* | mask *PORT MASK*] [*TCP-FLAG*] [cos *OUTER-COS* [*MASK*] [vlan *OUTER-VLAN* [*MASK*] [[precedence *PRECEDENCE* [*MASK*]] [tos *TOS* [*MASK*]] | dscp *DSCP* [*MASK*]] [time-range *PROFILE-NAME*]

[*SEQUENCE-NUMBER*] {permit | deny} udp {*SRC-IP-ADDR SRC-IP-WILDCARD* | host *SRC-IP-ADDR* | any} {*SRC-MAC-ADDR SRC-MAC-WILDCARD* | host *SRC-MAC-ADDR* | any} [{eq | lt | gt | neq} *PORT* | range *MIN-PORT MAX-PORT* | mask *PORT MASK*] {*DST-IP-ADDR DST-IP-WILDCARD* | host *DST-IP-ADDR* | any} {*DST-MAC-ADDR DST-MAC-WILDCARD* | host *DST-MAC-ADDR* | any} [{eq | lt | gt | neq} *PORT* | range *MIN-PORT MAX-PORT* | mask *PORT MASK*] [cos *OUTER-COS* [*MASK*] [vlan *OUTER-VLAN* [[precedence *PRECEDENCE* [*MASK*]] [tos *TOS* [*MASK*]] | dscp *DSCP* [*MASK*]] [time-range *PROFILE-NAME*]

[*SEQUENCE-NUMBER*] {permit | deny} icmp {*SRC-IP-ADDR SRC-IP-WILDCARD* | host *SRC-IP-ADDR* | any} {*SRC-MAC-ADDR SRC-MAC-WILDCARD* | host *SRC-MAC-ADDR* | any} {*DST-IP-ADDR DST-IP-WILDCARD* | host *DST-IP-ADDR* | any} {*DST-MAC-ADDR DST-MAC-WILDCARD* | host *DST-MAC-ADDR* | any} [*ICMP-TYPE* [*ICMP-CODE*] | *ICMP-MESSAGE*] [cos *OUTER-COS* [*MASK*] [vlan *OUTER-VLAN* [*MASK*] [[precedence *PRECEDENCE* [*MASK*]] [tos *TOS* [*MASK*]] | dscp *DSCP* [*MASK*]] [time-range *PROFILE-NAME*]

no *SEQUENCE-NUMBER*

Parameters

Parameters	Description
SEQUENCE-NUMBER	Specifies the sequence number. The range is from 1 to 65535. The lower the number is, the higher the priority of the permit/deny rule.

Parameters	Description
PROTOCOL	(Optional) Specifies the IP protocol ID or one of the following protocol names. Available protocol names are **eigrp**, **esp**, **gre**, **igmp**, **ospf**, **pim**, **vrrp**, **pcp** and **ipinip**. If the protocol ID is specified, the *MASK* (0x0-0xff) parameter is optional. The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
cos *OUTER-COS*	(Optional) Specifies the outer priority value. This value must be between 0 and 7.
MASK	(Optional) Specifies the outer priority mask (0x0-0x7). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
vlan *OUTER-VLAN*	(Optional) Specifies the outer VLAN ID.
MASK	(Optional) Specifies the outer VLAN ID mask (0x0-0xfff). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
any	Specifies to use any source MAC address, any destination MAC address, any source IP address, or any destination IP address.
host *SRC-MAC-ADDR*	Specifies a specific source host MAC address.
SRC-MAC-ADDR SRC-MAC-WILDCARD	Specifies a group of source MAC addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to bit value 0 will be checked.
host *DST-MAC-ADDR*	Specifies a specific destination host MAC address.
DST-MAC-ADDR DST-MAC-WILDCARD	Specifies a group of destination MAC addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
host *SRC-IP-ADDR*	Specifies a specific source host IP address.
SRC-IP-ADDR SRC-IP-WILDCARD	Specifies a group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
host *DST-IP-ADDR*	Specifies a specific destination host IP address.
DST-IP-ADDR DST-IP-WILDCARD	Specifies a group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
precedence *PRECEDENCE*	(Optional) Specifies that packets can be filtered by precedence level, as specified by a number from 0 to 7.
MASK	(Optional) Specifies the precedence mask (0x0-0x7). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.

Parameters	Description
tos *TOS*	(Optional) Specifies that packets can be filtered by type of service level, as specified by a number from 0 to 15.
MASK	(Optional) Specifies the ToS mask (0x0-0xf). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
dscp *DSCP*	(Optional) Specifies the matching DSCP code in the IP header. The range is from 0 to 63, or select the following DSCP name: af11 - 001010, af12 -001100, af13 - 001110, af21 - 010010, af22 - 010100, af23 - 010110, af31 - 011010, af32 - 011100, af33 - 011110, af41 - 100010, af42 - 100100, af43 - 100110, cs1 - 001000, cs2 - 010000, cs3 - 011000, cs4 - 100000, cs5 - 101000, cs6 - 110000, cs7 - 111000, default - 000000, ef – 101110.
MASK	(Optional) Specifies the DSCP mask (0x0-0x3f). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
lt *PORT*	(Optional) Specifies to match if less than the specified port number.
gt *PORT*	(Optional) Specifies to match if greater than the specified port number.
eq *PORT*	(Optional) Specifies to match if equal to the specified port number.
neq *PORT*	(Optional) Specifies to match if not equal to the specified port number.
range *MIN-PORT MAX-PORT*	(Optional) Specifies to match if falling within the specified range of ports.
mask *PORT MASK*	(Optional) Specifies to match ports defined by the mask. The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
TCP-FLAG	(Optional) Specifies the TCP flag fields and the specified TCP header bits called **ack** (acknowledge), **fin** (finish), **psh** (push), **rst** (reset), **syn** (synchronize), or **urg** (urgent).
fragments	(Optional) Specifies the packet fragment's filtering.
time-range *PROFILE-NAME*	(Optional) Specifies the name of time period profile associated with the access list delineating its activation period.
ICMP-TYPE	(Optional) Specifies the ICMP message type. The valid number for the message type is from 0 to 255.
ICMP-CODE	(Optional) Specifies the ICMP message code. The valid number for the message code is from 0 to 255.

Parameters	Description
ICMP-MESSAGE	(Optional) Specifies the ICMP message. The following pre-defined parameters are available for selection: beyond-scope, destination-unreachable, echo-reply, echo-request, header, hop-limit, mld-query, mld-reduction, mld-report, nd-na, nd-ns, next-header, no-admin, no-route, packet-too-big, parameter-option, parameter-problem, port-unreachable, reassembly-timeout, redirect, renum-command, renum-result, renum-seq-number, router-advertisement, router-renumbering, router-solicitation, time-exceeded, unreachable.

Default

None

Command Mode

Extended Expert Access-list Configuration Mode.

Command Default Level

Level: 12

Usage Guideline

If a rule entry is created without a sequence number, a sequence number will be automatically assigned. If it is the first entry, the sequence number 10 is assigned. A subsequent rule entry will be assigned a sequence number that is 10 greater than the largest sequence number in that access list and is placed at the end of the list.
The user can use the **access-list resequence** command to change the start sequence number and the increment number of entries for the specified access list. After the command is applied, new entries without any specified sequence number will be assigned a number based on the new sequence setting of the specified access list.
When you manually assign the sequence number, it is better to have a reserved interval for future lower sequence number entries. Otherwise, it will be more difficult to insert an entry with a lower sequence number.
The sequence number must be unique in the domain of an access list. If you enter a sequence number that is already present, an error message will be shown.

Rules with the TCP/UDP port range field can only be assigned to ingress interfaces. If the access-list is assigned to the egress interface, rules that are for this access-list and with the TCP/UDP port range field will be ignored.

Example

This example shows how to use the extended expert ACL. The purpose is to deny all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 00:13:00:49:82:72.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# expert access-list extended exp_acl
GA-MLxxTPoE+(config-exp-nacl)# deny tcp host 192.168.4.12 host 0013.0049.8272 any any
GA-MLxxTPoE+(config-exp-nacl)#
```

5.1.18 permit | deny (ip access-list)

This command is used to add a permit or a deny entry. Use the **no** form of the command to remove an entry.

Syntax

Extended Access List:

[*SEQUENCE-NUMBER*] {**permit** | **deny**} **tcp** {**any** | **host** *SRC-IP-ADDR* | *SRC-IP-ADDR SRC-IP-WILDCARD*} [{**eq** | **lt** | **gt** | **neq**} *PORT* | **range** *MIN-PORT MAX-PORT* | **mask** *PORT MASK*] {**any** | **host** *DST-IP-ADDR* | *DST-IP-ADDR DST-IP-WILDCARD*} [{**eq** | **lt** | **gt** | **neq**} *PORT* | **range** *MIN-PORT MAX-PORT* | **mask** *PORT MASK*] [*TCP-FLAG*] [[**precedence** *PRECEDENCE* [*MASK*]] [**tos** *TOS* [*MASK*]] | **dscp** *DSCP* [*MASK*]] [**time-range** *PROFILE-NAME*]

[*SEQUENCE-NUMBER*] {**permit** | **deny**} **udp** {**any** | **host** *SRC-IP-ADDR* | *SRC-IP-ADDR SRC-IP-WILDCARD*} [{**eq** | **lt** | **gt** | **neq**} *PORT* | **range** *MIN-PORT MAX-PORT* | **mask** *PORT MASK*] {**any** | **host** *DST-IP-ADDR* | *DST-IP-ADDR DST-IP-WILDCARD*} [{**eq** | **lt** | **gt** | **neq**} *PORT* | **range** *MIN-PORT MAX-PORT* | **mask** *PORT MASK*] [[**precedence** *PRECEDENCE* [*MASK*]] [**tos** *TOS* [*MASK*]] | **dscp** *DSCP* [*MASK*]] [**time-range** *PROFILE-NAME*]

[*SEQUENCE-NUMBER*] {**permit** | **deny**} **icmp** {**any** | **host** *SRC-IP-ADDR* | *SRC-IP-ADDR SRC-IP-WILDCARD*} {**any** | **host** *DST-IP-ADDR* | *DST-IP-ADDR DST-IP-WILDCARD*} [*ICMP-TYPE* [*ICMP-CODE*] | *ICMP-MESSAGE*] [[**precedence** *PRECEDENCE* [*MASK*]] [**tos** *TOS* [*MASK*]] | **dscp** *DSCP* [*MASK*]] [**time-range** *PROFILE-NAME*]

[*SEQUENCE-NUMBER*] {permit | deny} {gre | esp | eigrp | igmp | ipinip | ospf | pcp | pim | vrrp | protocol-id *PROTOCOL-ID* [*MASK*]} {any | host *SRC-IP-ADDR* | *SRC-IP-ADDR SRC-IP-WILDCARD*} {any | host *DST-IP-ADDR* | *DST-IP-ADDR DST-IP-WILDCARD*} [fragments] [[precedence *PRECEDENCE* [*MASK*]] [tos *TOS* [*MASK*]] | dscp *DSCP* [*MASK*]] [time-range *PROFILE-NAME*]

[*SEQUENCE-NUMBER*] {permit | deny} {any | host *SRC-IP-ADDR* | *SRC-IP-ADDR SRC-IP-WILDCARD*} [any | host *DST-IP-ADDR* | *DST-IP-ADDR DST-IP-WILDCARD*] [fragments] [[precedence *PRECEDENCE* [*MASK*]] [tos *TOS* [*MASK*]] | dscp *DSCP* [*MASK*]] [time-range *PROFILE-NAME*]

Standard IP Access List:

[*SEQUENCE-NUMBER*] {permit | deny} {any | host *SRC-IP-ADDR* | *SRC-IP-ADDR SRC-IP-WILDCARD*} [any | host *DST-IP-ADDR* | *DST-IP-ADDR DST-IP-WILDCARD*] [time-range *PROFILE-NAME*]

no *SEQUENCE-NUMBER*

Parameters

Parameters	Description
SEQUENCE-NUMBER	Specifies the sequence number. The range is from 1 to 65535. The lower the number is, the higher the priority of the permit/deny rule.
any	Specifies any source IP address or any destination IP address.
host *SRC-IP-ADDR*	Specifies a specific source host IP address.
SRC-IP-ADDR SRC-IP-WILDCARD	Specifies a group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
host *DST-IP-ADDR*	Specifies a specific destination host IP address.
DST-IP-ADDR DST-IP-WILDCARD	Specifies a group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
precedence *PRECEDENCE*	(Optional) Specifies that packets can be filtered by precedence level, as specified by a number from 0 to 7.
MASK	(Optional) Specifies the precedence mask (0x0-0x7). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.

Parameters	Description
dscp *DSCP*	(Optional) Specifies the matching DSCP code in the IP header. The range is from 0 to 63, or select the following DSCP name: af11 - 001010, af12 -001100, af13 - 001110, af21 - 010010, af22 - 010100, af23 - 010110, af31 - 011010, af32 - 011100, af33 - 011110, af41 - 100010, af42 - 100100, af43 - 100110, cs1 - 001000, cs2 - 010000, cs3 - 011000, cs4 - 100000, cs5 - 101000, cs6 - 110000, cs7 - 111000, default - 000000, ef – 101110.
MASK	(Optional) Specifies the DSCP mask (0x0-0x3f). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
tos *TOS*	(Optional) Specifies that packets can be filtered by type of service level, as specified by a number from 0 to 15.
MASK	(Optional) Specifies the ToS mask (0x0-0xf). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
lt *PORT*	(Optional) Specifies to match if less than the specified port number.
gt *PORT*	(Optional) Specifies to match if greater than the specified port number.
eq *PORT*	(Optional) Specifies to match if equal to the specified port number.
neq *PORT*	(Optional) Specifies to match if not equal to the specified port number.
range *MIN-PORT MAX-PORT*	(Optional) Specifies to match if falling within the specified range of ports.
mask *PORT MASK*	(Optional) Specifies to match ports defined by the mask. The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
TCP-FLAG	(Optional) Specifies the TCP flag fields and the specified TCP header bits called **ack** (acknowledge), **fin** (finish), **psh** (push), **rst** (reset), **syn** (synchronize), or **urg** (urgent).
fragments	(Optional) Specifies the packet fragment's filtering
time-range *PROFILE-NAME*	(Optional) Specifies the name of the time period profile associated with the access list delineating its activation period.
tcp, udp, igmp, ipinip, gre, esp, eigrp, ospf, pcp, pim, vrrp	Specifies Layer 4 protocols.
PROTOCOL-ID	(Optional) Specifies the protocol ID. The valid value is from 0 to 255.
MASK	(Optional) Specifies the protocol ID mask (0x0-0xff). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.

Parameters	Description
ICMP-TYPE	(Optional) Specifies the ICMP message type. The valid number for the message type is from 0 to 255.
ICMP-CODE	(Optional) Specifies the ICMP message code. The valid number for the message code is from 0 to 255.
ICMP-MESSAGE	(Optional) Specifies the ICMP message. The pre-defined parameters are available for selection: administratively-prohibited,alternate-address,conversion-error,host-prohibited,net-prohibited,echo,echo-reply,pointer-indicates-error,host-isolated,host-precedence-violation,host-redirect,host-tos-redirect,host-tos-unreachable,host-unknown,host-unreachable, information-reply,information-request,mask-reply,mask-request,mobile-redirect,net-redirect,net-tos-redirect,net-tos-unreachable, net-unreachable,net-unknown,bad-length,option-missing,packet-fragment,parameter-problem,port-unreachable,precedence-cutoff, protocol-unreachable,reassembly-timeout,redirect-message,router-advertisement,router-solicitation,source-quench,source-route-failed, time-exceeded,timestamp-reply,timestamp-request,traceroute,ttl-expired,unreachable.

Default

None

Command Mode

IP Access-list Configuration Mode.

Command Default Level

Level: 12

Usage Guideline

If a rule entry is created without a sequence number, a sequence number will be automatically assigned. If it is the first entry, the sequence number 10 is assigned. A subsequent rule entry will be assigned a sequence number that is 10 greater than the largest sequence number in that access list and is placed at the end of the list.

The user can use the **access-list resequence** command to change the start sequence number and the increment number of entries for the specified access list. After the command is applied, new entries without any specified sequence number will be assigned a number based on the new sequence setting of the specified access list.
When you manually assign the sequence number, it is better to have a reserved interval for future lower sequence number entries. Otherwise, it will be more difficult to insert an entry with a lower sequence number.
The sequence number must be unique in the domain of an access list. If you enter a sequence number that is already present, an error message will be shown.
To create a matching rule for an IP standard access list, only the source IP address or destination IP address fields can be specified.

Example

This example shows how to create four entries for an IP extended access list, named Strict-Control. These entries are: permit TCP packets destined for network 10.20.0.0, permit TCP packets destined for host 10.100.1.2, permit all TCP packets go to TCP destination port 80 and permit all ICMP packets.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip access-list extended Strict-Control
GA-MLxxTPoE+(config-ip-ext-acl)# permit tcp any 10.20.0.0 0.0.255.255
GA-MLxxTPoE+(config-ip-ext-acl)# permit tcp any host 10.100.1.2
GA-MLxxTPoE+(config-ip-ext-acl)# permit tcp any any eq 80
GA-MLxxTPoE+(config-ip-ext-acl)# permit icmp any any
GA-MLxxTPoE+(config-ip-ext-acl)#
```

This example shows how to create two entries for an IP standard access list, named “std-acl”. These entries are: permit IP packets destined for network 10.20.0.0, permit IP packets destined for host 10.100.1.2.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip access-list std-acl
GA-MLxxTPoE+(config-ip-acl)# permit any 10.20.0.0 0.0.255.255
GA-MLxxTPoE+(config-ip- acl)# permit any host 10.100.1.2
GA-MLxxTPoE+(config-ip- acl)#
```

5.1.19 permit | deny (ipv6 access-list)

This command is used to add a permit entry or deny entry to the IPv6 access list. Use the **no** form of this command to remove an entry from the IPv6 access list.

Syntax

Extended IPv6 Access List:

[*SEQUENCE-NUMBER*] {permit | deny} tcp {any | host *SRC-IPV6-ADDR* | *SRC-IPV6-ADDR/PREFIX-LENGTH*} [{eq | lt | gt | neq} *PORT* | range *MIN-PORT MAX-PORT* | mask *PORT MASK*] {any | host *DST-IPV6-ADDR* | *DST-IPV6-ADDR/PREFIX-LENGTH*} [{eq | lt | gt | neq} *PORT* | range *MIN-PORT MAX-PORT* | mask *PORT MASK*] [*TCP-FLAG*] [dscp *VALUE* [*MASK*] | traffic-class *VALUE* [*MASK*]] [flow-label *FLOW-LABEL* [*MASK*]] [time-range *PROFILE-NAME*]

[*SEQUENCE-NUMBER*] {permit | deny} udp {any | host *SRC-IPV6-ADDR* | *SRC-IPV6-ADDR/PREFIX-LENGTH*} [{eq | lt | gt | neq} *PORT* | range *MIN-PORT MAX-PORT* | mask *PORT MASK*] {any | host *DST-IPV6-ADDR* | *DST-IPV6-ADDR/PREFIX-LENGTH*} [{eq | lt | gt | neq} *PORT* | range *MIN-PORT MAX-PORT* | mask *PORT MASK*] [dscp *VALUE* [*MASK*] | traffic-class *VALUE* [*MASK*]] [flow-label *FLOW-LABEL* [*MASK*]] [time-range *PROFILE-NAME*]

[*SEQUENCE-NUMBER*] {permit | deny} icmp {any | host *SRC-IPV6-ADDR* | *SRC-IPV6-ADDR/PREFIX-LENGTH*} {any | host *DST-IPV6-ADDR* | *DST-IPV6-ADDR/PREFIX-LENGTH*} [*ICMP-TYPE* [*ICMP-CODE*] | *ICMP-MESSAGE*] [dscp *VALUE* [*MASK*] | traffic-class *VALUE* [*MASK*]] [flow-label *FLOW-LABEL* [*MASK*]] [time-range *PROFILE-NAME*]

[*SEQUENCE-NUMBER*] {permit | deny} {esp | pcp | sctp | protocol-id *PROTOCOL-ID* [*MASK*]} {any | host *SRC-IPV6-ADDR* | *SRC-IPV6-ADDR/PREFIX-LENGTH*} {any | host *DST-IPV6-ADDR* | *DST-IPV6-ADDR/PREFIX-LENGTH*} [fragments] [dscp *VALUE* [*MASK*] | traffic-class *VALUE* [MASK]] [flow-label *FLOW-LABEL* [*MASK*]] [time-range *PROFILE-NAME*]

[*SEQUENCE-NUMBER*] {permit | deny} {any | host *SRC-IPV6-ADDR* | *SRC-IPV6-ADDR/PREFIX-LENGTH*} [any | host *DST-IPV6-ADDR* | *DST-IPV6-ADDR/PREFIX-LENGTH*] [fragments] [dscp *VALUE* [*MASK*] | traffic-class *VALUE* [*MASK*]] [flow-label *FLOW-LABEL* [*MASK*]] [time-range *PROFILE-NAME*]

Standard IPv6 Access List:

[*SEQUENCE-NUMBER*] {permit | deny} {any | host *SRC-IPV6-ADDR* | *SRC-IPV6-ADDR/PREFIX-LENGTH*} [any | host *DST-IPV6-ADDR* | *DST-IPV6-ADDR/PREFIX-LENGTH*] [time-range *PROFILE-NAME*]

no *SEQUENCE-NUMBER*

Parameters

Parameters	Description
SEQUENCE-NUMBER	Specifies the sequence number. The range is from 1 to 65535. The lower the number is, the higher the priority of the permit/deny rule.
any	Specifies any source IPv6 address or any destination IPv6 address.
host *SRC-IPV6-ADDR*	Specifies a specific source host IPv6 address.
SRC-IPV6-ADDR/PREFIX-LENGTH	Specifies a source IPv6 network.
host *DST-IPV6-ADDR*	Specifies a specific destination host IPv6 address.
DST-IPV6-ADDR/PREFIX-LENGTH	Specifies a destination IPv6 network.
tcp, udp, icmp, esp, pcp, sctp	Specifies the Layer 4 protocol type.
dscp *VALUE*	(Optional) Specifies the matching traffic class value in IPv6 header. The range is from 0 to 63, or select the following DSCP name: af11 - 001010, af12 -001100, af13 - 001110, af21 - 010010, af22 - 010100, af23 - 010110, af31 - 011010, af32 - 011100, af33 - 011110, af41 - 100010, af42 - 100100, af43 - 100110, cs1 - 001000, cs2 - 010000, cs3 - 011000, cs4 - 100000, cs5 - 101000, cs6 - 110000, cs7 - 111000, default - 000000, ef – 101110.
MASK	(Optional) Specifies the DSCP mask (0x0-0x3f). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
traffic-class *VALUE*	(Optional) Specifies the matching traffic class value in the IPv6 header. The range is from 0 to 255.
MASK	(Optional) Specifies the traffic class mask (0x0-0xff). If not specified, 0xff is used.
lt *PORT*	(Optional) Specifies to match if less than the specified port number.
gt *PORT*	(Optional) Specifies to match if greater than the specified port number.
eq *PORT*	(Optional) Specifies to match if equal to the specified port number.
neq *PORT*	(Optional) Specifies to match if not equal to the specified port number.
range *MIN-PORT MAX-PORT*	(Optional) Specifies to match if falling within the specified range of ports.
mask *PORT MASK*	(Optional) Specifies to match ports defined by the mask. The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.

Parameters	Description
PROTOCOL-ID	(Optional) Specifies the protocol ID. The valid value is from 0 to 255.
MASK	(Optional) Specifies the protocol ID mask (0x0-0xff). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
ICMP-TYPE	(Optional) Specifies the ICMP message type. The valid number of the message type is from 0 to 255.
ICMP-CODE	(Optional) Specifies the ICMP message code. The valid number of the code type is from 0 to 255.
ICMP-MESSAGE	(Optional) Specifies the ICMP message. The following pre-defined parameters are available for selection: beyond-scope, destination-unreachable, echo-reply, echo-request, erroneous_header, hop-limit, multicast-listener-query, multicast-listener-done, multicast-listener-report, nd-na, nd-ns, next-header, no-admin, no-route, packet-too-big, parameter-option, parameter-problem, port-unreachable, reassembly-timeout, redirect, renum-command, renum-result, renum-seq-number, router-advertisement, router-renumbering, router-solicitation, time-exceeded, unreachable.
TCP-FLAG	(Optional) Specifies the TCP flag fields and the specified TCP header bits called **ack** (acknowledge), **fin** (finish), **psh** (push), **rst** (reset), **syn** (synchronize), or **urg** (urgent).
flow-label *FLOW-LABEL*	(Optional) Specifies the flow label value, within the range of 0 to 1048575.
MASK	(Optional) Specifies the flow label mask (0x0-0xfffff). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
fragments	(Optional) Specifies the packet fragment's filtering
time-range *PROFILE-NAME*	(Optional) Specifies the name of time period profile associated with the access list delineating its activation period.

Default

None

Command Mode

IPv6 Access-list Configuration Mode.

Command Default Level

Level: 12

Usage Guideline

If a rule entry is created without a sequence number, a sequence number will be automatically assigned. If it is the first entry, the sequence number 10 is assigned. A subsequent rule entry will be assigned a sequence number that is 10 greater than the largest sequence number in that access list and is placed at the end of the list.
The user can use the **access-list resequence** command to change the start sequence number and the increment number of entries for the specified access list. After the command is applied, new entries without any specified sequence number will be assigned a number based on the new sequence setting of the specified access list.
When you manually assign the sequence number, it is better to have a reserved interval for future lower sequence number entries. Otherwise, it will be more difficult to insert an entry with a lower sequence number.
The sequence number must be unique in the domain of an access list. If you enter a sequence number that is already present, an error message will be shown.

Example

This example shows how to create four entries for an IPv6 extended access list named “ipv6-control”. These entries are: permit TCP packets destined for network ff02::0:2/16, permit TCP packets destined for host ff02::1:2, permit all TCP packets go to port 80, and permit all ICMP packets.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ipv6 access-list extended ipv6-control
GA-MLxxTPoE+(config-ipv6-ext-acl)# permit tcp any ff02::0:2/16
GA-MLxxTPoE+(config-ipv6-ext-acl)# permit tcp any host ff02::1:2
GA-MLxxTPoE+(config-ipv6-ext-acl)# permit tcp any any eq 80
GA-MLxxTPoE+(config-ipv6-ext-acl)# permit icmp any any
GA-MLxxTPoE+(config-ipv6-ext-acl)#
```

This example shows how to create two entries for an IPv6 standard access-list named “ipv6-std-control”. These entries are: permit IPv6 packets destined for network ff02::0:2/16, and permit IPv6 packets destined for host ff02::1:2.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ipv6 access-list ipv6-std-control
GA-MLxxTPoE+(config-ipv6-acl)# permit any ff02::0:2/16
GA-MLxxTPoE+(config-ipv6-acl)# permit any host ff02::1:2
GA-MLxxTPoE+(config-ipv6-acl)#
```

5.1.20 permit | deny (mac access-list)

This command is used to define the rule for packets that will be permitted or denied. Use the **no** form command to remove an entry

Syntax

[*SEQUENCE-NUMBER*] {**permit** | **deny**} {**any** | **host** *SRC-MAC-ADDR* | *SRC-MAC-ADDR SRC-MAC-WILDCARD*} {**any** | **host** *DST-MAC-ADDR* | *DST-MAC-ADDR DST-MAC-WILDCARD*} [**ethernet-type** *TYPE MASK* [**cos** *VALUE* [*MASK*] [**vlan** *VLAN-ID* [*MASK*] [**time-range** *PROFILE-NAME*]

no *SEQUENCE-NUMBER*

Parameters

Parameters	Description
SEQUENCE-NUMBER	Specifies the sequence number. The range is from 1 to 65535. The lower the number is, the higher the priority of the permit/deny rule.
any	Specifies any source MAC address or any destination MAC address.
host *SRC-MAC-ADDR*	Specifies a specific source host MAC address.
SRC-MAC-ADDR SRC-MAC-WILDCARD	Specifies a group of source MAC addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
host *DST-MAC-ADDR*	Specifies a specific destination host MAC address.
DST-MAC-ADDR DST-MAC-WILDCARD	Specifies a group of destination MAC addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
ethernet-type *TYPE MASK*	(Optional) Specifies that the Ethernet type which is a hexadecimal number from 0 to FFFF or the name of an Ethernet type which can be one of the following: aarp, appletalk, decnet-iv, etype-6000, etype-8042, lat, lavc-sca, mop-console, mop-dump, vines-echo, vines-ip, xns-idp, or arp.
cos *VALUE*	(Optional) Specifies the priority value of 0 to 7.
MASK	(Optional) Specifies the outer priority mask (0x0-0x7). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
vlan *VLAN-ID*	(Optional) Specifies the VLAN-ID.
MASK	(Optional) Specifies the outer VLAN ID mask (0x0-0x0fff). If not specified, 0x0fff is used.
time-range *PROFILE-NAME*	(Optional) Specifies the name of time period profile associated with the access list delineating its activation period

Default

None

Command Mode

MAC Access-list Configuration Mode.

Command Default Level

Level: 12

Usage Guideline

If a rule entry is created without a sequence number, a sequence number will be automatically assigned. If it is the first entry, the sequence number 10 is assigned. A subsequent rule entry will be assigned a sequence number that is 10 greater than the largest sequence number in that access list and is placed at the end of the list.
The user can use the command access-list sequence to change the start sequence number and increment number for the specified access list. After the command is applied, the new rule without specified sequence number will be assigned sequence based new sequence setting of the specified access list.
When you manually assign the sequence number, it is better to have a reserved interval for future lower sequence number entries. Otherwise, it will create extra effort to insert an entry with a lower sequence number.
The sequence number must be unique in the domain of an access-list. If you enter a sequence number that is already present, an error message will be displayed.
Rules with the TCP/UDP port range field can only be assigned to ingress interfaces. If the access-list is assigned to the egress interface, the rules that are for this access-list and with the TCP/UDP port range field will be ignored.
Multiple entries can be added to the list, and you can use permit for one entry and use deny for the other entry. Different permit and deny commands can match different fields available for setting.

Example

This example shows how to configure MAC access entries in the profile daily-profile to allow two sets of source MAC addresses.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# mac access-list extended daily-profile
GA-MLxxTPoE+(config-mac-ext-acl)# permit 00:50:40:00:00:00  00:00:00:ff:ff:ff any
GA-MLxxTPoE+(config-mac-ext-acl)# permit 00:f4:57:00:00:00 00:00:00:ff:ff:ff any
GA-MLxxTPoE+(config-mac-ext-acl)#
```

5.1.21 show access-group

This command is used to display access group information for interface(s).

Syntax

- **show access-group [interface** *INTERFACE-ID*]

Parameters

Parameters	Description
interface *INTERFACE-ID*	(Optional) Specifies the interface to be displayed.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

If interface is not specified, all of the interfaces that have access list configured will be displayed.

Example

This example shows how to display access lists that are applied to all of the interfaces.

```
GA-MLxxTPoE+# show access-group

Gi1/0/2:
  Inbound expert access-list : exp_acl(ID: 9999)
Gi1/0/3:
  Inbound ipv6 access-list  : ip6-control(ID: 14999)
Gi1/0/4:
  Inbound mac access-list    : daily-profile(ID: 7999)

GA-MLxxTPoE+#
```

5.1.22 show access-list

This command is used to display the access list configuration information.

Syntax

- **show access-list** [**ip** [*NAME* | *NUMBER*] | **mac** [*NAME* | *NUMBER*] | **ipv6** [*NAME* | *NUMBER*] | **expert** [*NAME* | *NUMBER*] | **arp** [*NAME*]]

Parameters

Parameters	Description
ip	(Optional) Specifies to display a listing of all IP access lists.
mac	(Optional) Specifies to display a listing of all MAC access lists.
ipv6	(Optional) Specifies to display a listing of all IPv6 access lists.
expert	(Optional) Specifies to display a listing of all expert access lists.
arp	(Optional) Specifies to display the ARP access list.
NAME	(Optional) Specifies to the name of the access list to be displayed.
NUMBER	(Optional) Specifies to the ID of the access list to be displayed.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command displays access list information. If no option is specified, a listing of all configured access lists is displayed. If the type of access list is specified, detailed information of the access list will be displayed. If the user enables the ACL hardware counter for an access list, the counter will be displayed based on each access list entry.

Example

This example shows how to display all access lists.

```
GA-MLxxTPoE+#show access-list

Access-List-Name                                Type
----------------------------------------   ---------------
trict-Control(ID: 3999)                    ip ext-acl
daily-profile(ID: 7999)                    mac ext-acl
exp_acl(ID: 9999)                          expert ext-acl
ip6-control(ID: 14999)                     ipv6 ext-acl

Total Entries: 4


GA-MLxxTPoE+#
```

This example shows how to display the IP access list called Strict-Control.

```
GA-MLxxTPoE+#show access-list ip Strict-Control

Extended IP access list Strict-Control(ID: 3999)
    10 permit any 10.20.0.0 0.0.255.255
    20 permit any host 10.100.1.2

GA-MLxxTPoE+#
```

5.1.23 show vlan access-map

This command is used to display the VLAN access-map configuration information.

Syntax

- **show vlan access-map** [*MAP-NAME*]

Parameters

Parameters	Description
MAP-NAME	(Optional) Specifies the name of the VLAN access map being configured. The name can be up to 32 characters.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

If no access-map name is specified, all VLAN access-map information will be displayed. If the user enables the ACL hardware counter for an access-map, the counter will be displayed based on each sub-map.

Example

This example shows how to display the VLAN access-map.

```
GA-MLxxTPoE+#show vlan access-map

VLAN access-map vlan-map 10
  match ip access list: stp_ip1(ID: 1888)
action: forward
VLAN access-map vlan-map 20
  match mac access list: ext_mac(ID: 6995)
  action: redirect Gi1/0/5

GA-MLxxTPoE+#
```

5.1.24 show vlan filter

This command is used to display the VLAN filter configuration of VLAN interfaces.

Syntax

- **show vlan filter [access-map** *MAP-NAME* **| vlan** *VLAN-ID*]

Parameters

Parameters	Description
access-map *MAP-NAME*	(Optional) Specifies the name of the VLAN access map. The name can be up to 32 characters.
vlan *VLAN-ID*	(Optional) Specifies the VLAN ID.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

The **show vlan filter access-map** command is used to display the VLAN filter information by access map. The command **show vlan filter vlan** is used to display the VLAN filter information by VLAN.

Example

This example shows how to display VLAN filter information.

```
GA-MLxxTPoE+# show vlan filter

VLAN Map aa
  Configured on VLANs: 5-127,221-333
VLAN Map bb
  Configured on VLANs: 1111-1222

GA-MLxxTPoE+#

GA-MLxxTPoE+# show vlan filter vlan 5

VLAN ID 5
  VLAN Access Map: aa

GA-MLxxTPoE+#
```

5.1.25 vlan access-map

This command is used to create a sub-map of a VLAN access map and enter the VLAN access-map sub-map configure mode. Use the **no** form of this command to delete an access-map or its sub-map.

Syntax

- **vlan access-map** *MAP-NAME* [*SEQUENCE-NUM*]
- **no vlan access-map** *MAP-NAME* [*SEQUENCE-NUM*]

Parameters

Parameters	Description
MAP-NAME	Specifies the name of the VLAN access map to be configured. The name can be up to 32 characters.
SEQUENCE-NUM	(Optional) Specifies the sequence number of the sub-map. The valid range is from 1 to 65535.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

A VLAN access map can contain multiple sub-maps. For each sub-map, one access list (IP access list, IPv6 access list or MAC access list) can be specified and one action can be specified. After a VLAN access map is created, the user can use the **vlan filter** command to apply the access map to VLAN(s).
A sequence number will be assigned automatically if the user does not assign it manually, and the automatically assigned sequence number starts from 10, and increase 10 per new entry.
The packet that matches the sub-map (that is packet permitted by the associated access-list) will take the action specified for the sub-map. No further check against the next sub-maps is done. If the packet does not match a sub-map, then the next sub-map will be checked.
Using the **no** form of this command without specify sequence numbers, will delete all sub-map information of the specified access-map.

Example

This example shows how to create a VLAN access map.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan access-map vlan-map 20
GA-MLxxTPoE+(config-access-map)#
```

5.1.26 vlan filter

This command is used to apply a VLAN access map in a VLAN. Use the **no** form of this command to remove a VLAN access map from the VLAN.

Syntax

- **vlan filter** *MAP-NAME* **vlan-list** *VLAN-ID-LIST*
- **no vlan filter** *MAP-NAME* **vlan-list** *VLAN-ID-LIST*

Parameters

Parameters	Description
MAP-NAME	Specifies the name of the VLAN access map.
vlan-list *VLAN-ID-LIST*	Specifies the VLAN ID list.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

A VLAN can only be associated with one VLAN access map.

Example

This example shows how to apply the VLAN access-map “vlan-map” in VLAN 5.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan filter vlan-map vlan-list 5
GA-MLxxTPoE+(config-access-map)# end
GA-MLxxTPoE+# show vlan filter

VLAN Map vlan-map
  Configured on VLANs: 5

GA-MLxxTPoE+#
```

5.2 QoS (Quality of Service) Commands

QoS (Quality of Service) is a function to allocate the optimum bandwidth according to the communication purpose to secure response time and throughput required for each communication.
It performs communication priority control based on the priority tag (priority information) added to the header of a receive packet.
It also allows to restrict bandwidth according to the priority tag for each port.

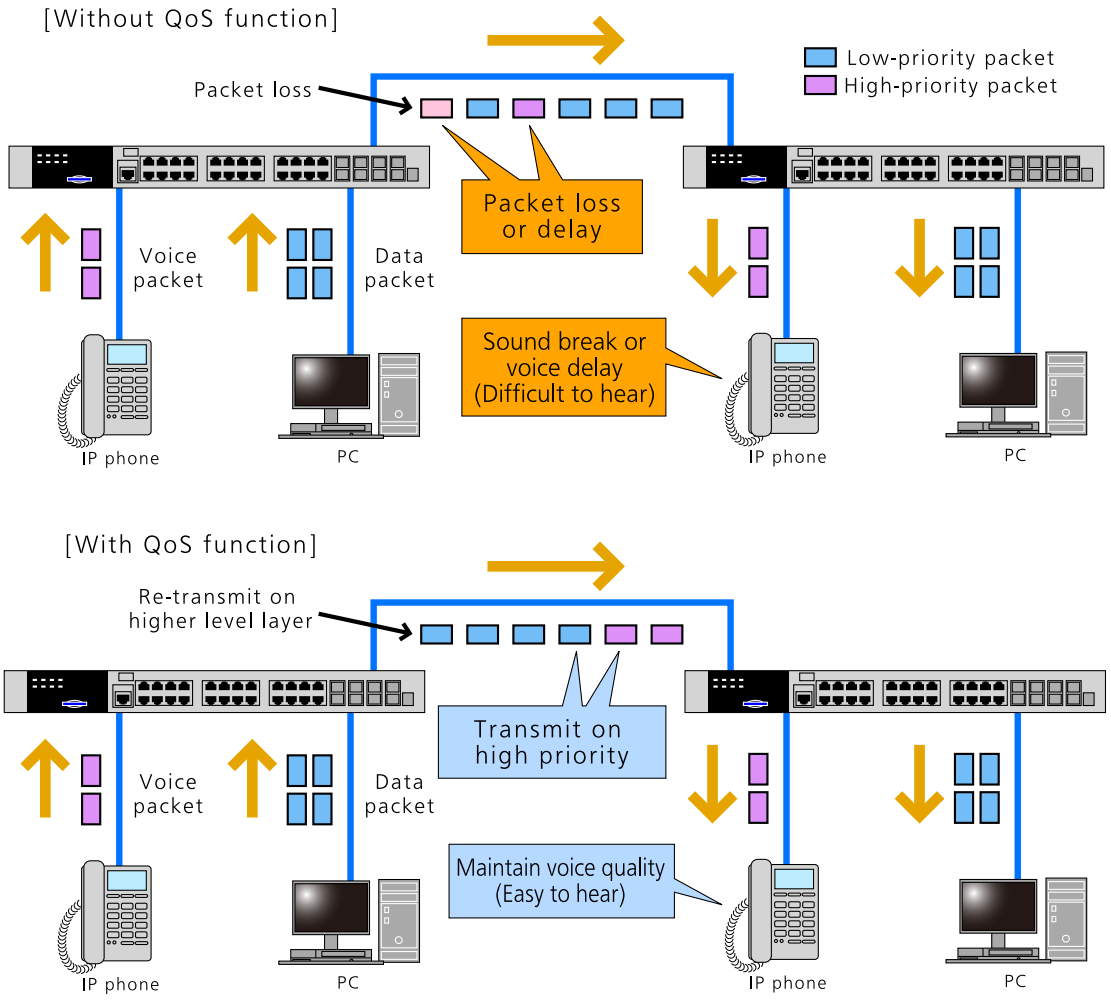


Figure 41-1 QoS overview

5.2.1 class

This command is used to specify the name of the class map to be associated with a traffic policy and then enter into policy map class configuration mode. Use the **no** form of this command to remove the policy definition for the specified class.

Syntax

- **class** *NAME*
- **no class** *NAME*
- **class class-default**

Parameters

Parameters	Description
NAME	Specifies the name of the class map to be associated with a traffic policy.

Default

None

Command Mode

Policy-map Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

This command enters the policy-map class configuration mode. All the traffic that does not match the proceeding defined class will be classified as class-default. If the specified name of class map does not exist, no traffic is classified to the class.

Example

This example shows how to define a policy map, policy1, which defines policies for the class “class-dscp-red”. The packets that match DSCP 10, 12, or 14 will all be marked as DSCP 10 and be policed by a single rate policer.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# class-map class-dscp-red
GA-MLxxTPoE+(config-cmap)# match ip dscp 10,12,14
GA-MLxxTPoE+(config-cmap)# exit
GA-MLxxTPoE+(config)# policy-map policy1
GA-MLxxTPoE+(config-pmap)# class class-dscp-red
GA-MLxxTPoE+(config-pmap-c)# set ip dscp 10
GA-MLxxTPoE+(config-pmap-c)# police 1000000 2000 exceed-action set-dscp-transmit 0
GA-MLxxTPoE+(config-pmap-c)#
```

5.2.2 class-map

This command is used to create or modify a class-map that defines the criteria for packet matching, or enter the Class-map Configuration mode. Use the **no** form of this command to remove an existing class map from the Switch.

Syntax

- **class-map [match-all | match-any]** *NAME*
- **no class-map** *NAME*

Parameters

Parameters	Description
match-all	(Optional) Specifies how to evaluate multiple match criteria. Multiple match statements in the class map will be evaluated based on the logical AND. If neither match-all nor match-any is specified, match-any is implied.
match-any	(Optional) Specifies how to evaluate multiple match criteria. Multiple match statements in the class map will be evaluated based on the logical OR. If neither match-all nor match-any is specified, match-any is implied.
NAME	Specifies the name of the class map with a maximum of 32 characters.

Default

By default, only class-default exists.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use this command to create or modify a class-map that defines the criteria for matching packets. This command enters the Class-map Configuration mode where match commands are entered to define the match criteria for this class. When multiple match commands are defined for a class, use the **match-all** or **match-any** keyword to specify whether to evaluate the multiple match criteria based on either the logical AND or the logical OR.

Example

This example shows how to configure the "class_home_user "as the name of a class map. In this class map, a match statement specifies that the traffic that matches the access control list "acl_home_user" and matches the IPv6 protocol will be included under the class-map "class_home_user".

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# class-map match-all class_home_user
GA-MLxxTPoE+(config-cmap)# match access-group name acl_home_user
GA-MLxxTPoE+(config-cmap)# match protocol ipv6
GA-MLxxTPoE+(config-cmap)#
```

5.2.3 match

This command is used to define the match criteria for a class-map. Use the **no** form of this command to remove the match criteria.

Syntax

- **match {access-group name** *ACCESS-LIST-NAME* **| cos** *COS-LIST* **| [ip] dscp** *DSCP-LIST* **| [ip] precedence** *IP-PRECEDENCE-LIST* **| protocol** *PROTOCOL-NAME* **| vlan [***VLAN-LIST***}**
- **no match {access-group name** *ACCESS-LIST-NAME* **| cos** *COS-LIST* **| [ip] dscp** *DSCP-LIST* **| [ip] precedence** *IP-PRECEDENCE-LIST* **| protocol** *PROTOCOL-NAME* **| vlan** *VLAN-ID-LIST***}**

Parameters

Parameters	Description
access-group name *ACCESS-LIST-NAME*	Specifies an access list to be matched. Traffic that is permitted by the access list will be classified.
cos *COS-LIST*	Specifies a specific IEEE 802.1Q CoS value(s) to be matched. The *COS-LIST* parameter values are from 0 to 7. Enter one or more CoS values separated by commas or hyphen for a range list.
[ip] dscp *DSCP-LIST*	Specifies differentiated service code point values to be matched. Enter one or more differentiated service code point (DSCP) values separated by commas or hyphen for a range list. The valid range is from 0 to 63. **ip** - (Optional) Specifies that the match is for IPv4 packets only. If not specified, the match is for both IPv4 and IPv6 packets.
[ip] precedence *IP-PRECEDENCE-LIST*	Specifies IP precedence values to be matched. Enter one or more precedence values separated by commas or hyphen for a range list. The valid range is from 0 to 7. **ip** - (Optional) Specifies that the match is for IPv4 packets only. If not specified, the match is for both IP and IPv6 packets. For IPv6 packets, the precedence is most three significant bits of traffic class of IPv6 header.
protocol *PROTOCOL-NAME*	Specifies the protocol name to be matched.
vlan *VLAN-LIST*	Specifies the VLAN identification number, numbers, or range of numbers to be matched. Valid VLAN identification numbers must be in the range of 1 to 4094. Enter one or more VLAN values separated by commas or hyphens for a range list.

Default

None

Command Mode

Class-map Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

To use the **match** command, first enter the class-map command to specify the name of the class that will be used to establish the match criteria. The policy for handling these matched packets is defined in the policy-map class configuration mode.
The following lists the reference for the supported protocols for the match protocol command.

- **arp** - IP Address Resolution Protocol (ARP).
- **bgp** - Border Gateway Protocol.
- **dhcp** - Dynamic Host Configuration.
- **dns** - Domain Name Server lookup.
- **egp** - Exterior Gateway Protocol.
- **ftp** - File Transfer Protocol.
- **ip** - IP (version 4).
- **ipv6** - IP (version 6).
- **netbios** - NetBIOS.
- **nfs** - Network File System.
- **ntp** - Network Time Protocol.
- **ospf** - Open Shortest Path First.
- **pppoe** - Point-to-Point Protocol over Ethernet.
- **rip** - Routing Information Protocol.
- **rtsp** - Real-Time Streaming Protocol.
- **ssh** - Secured shell.
- **telnet** - Telnet.
- **tftp** - Trivial File Transfer Protocol.

Example

This example shows how to specify a class map called “class-home-user” and configures the access list named “acl-home-user” to be used as the match criterion for that class.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# class-map class-home-user
GA-MLxxTPoE+(config-cmap)# match access-group name acl-home-user
GA-MLxxTPoE+(config-cmap)#
```

This example shows how to specify a class map called “cos” and specifies that the CoS values of 1, 2, and 3 are match criteria for the class.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# class-map cos
GA-MLxxTPoE+(config-cmap)# match cos 1,2,3
GA-MLxxTPoE+(config-cmap)#
```

This example shows how classes called voice and video-n-data are created to classify traffic based on the CoS values. QoS treatment is then given to the appropriate packets in the cos-based-treatment policy map (in this example, the QoS treatment is a single rate policer and a two rate policer for class voice and video-n-data respectively). The service policy configured in this example is attached to GigabitEthernet1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# class-map voice
GA-MLxxTPoE+(config-cmap)# match cos 7
GA-MLxxTPoE+(config-cmap)# exit
GA-MLxxTPoE+(config)# class-map video-n-data
GA-MLxxTPoE+(config-cmap)# match cos 5
GA-MLxxTPoE+(config-cmap)# exit
GA-MLxxTPoE+(config)# policy-map cos-based-treatment
GA-MLxxTPoE+(config-pmap)# class voice
GA-MLxxTPoE+(config-pmap-c)# police 8000 1000 exceed-action drop
GA-MLxxTPoE+(config-pmap-c)# exit
GA-MLxxTPoE+(config-pmap)# class video-n-data
GA-MLxxTPoE+(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 exceed-
action set-dscp-transmit 2 violate-action drop
GA-MLxxTPoE+(config-pmap-c)# exit
GA-MLxxTPoE+(config-pmap)# exit
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# service-policy input cos-based-treatment
GA-MLxxTPoE+(config-if)#
```

5.2.4 mls qos aggregate-policer

This command is used to define a named aggregate policer for use in policy maps. Use the **no** form of this command to delete a named aggregate policer. The **mls qos aggregate-policer** command is for single rate policing and the **mls qos aggregate-policer cir** command is for two-rate policing.

Syntax

- **mls qos aggregate-policer** *NAME KBPS* [*BURST-NORMAL* [*BURST-MAX*]] [**conform-action** *ACTION*] **exceed-action** *ACTION* [**violate-action** *ACTION*] [**color-aware**]
- **mls qos aggregate-policer** *NAME* **cir** *CIR* [**bc** *CONFORM-BURST*] **pir** *PIR* [**be** *PEAK-BURST*] [**conform-action** *ACTION*] [**exceed-action** *ACTION* [**violate-action** *ACTION*]] [**color-aware**]
- **no mls qos aggregate-policer** *NAME*

Parameters

Parameters	Description
NAME	Specifies the name of the aggregate policing rule. The *NAME* parameter can be up to 32 characters, is case sensitive. The policer names must start with an alphabetic character (not a digit) and must be unique across all aggregate policers.
KBPS	Specifies the average rate, in kilobits per second.
BURST-NORMAL	(Optional) Specifies the normal burst size in kilobytes.
BURST-MAX	(Optional) Specifies the maximum burst size, in kilobytes.
CIR	Specifies the committed information rate in Kbps. The committed packet rate is the first token bucket for the two-rate metering.
PIR	Specifies the peak information rate in Kbps. The peak information rate is the second token bucket for the two-rate metering.
CONFORM-BURST	(Optional) Specifies the burst size for the first token bucket in kilobytes.
PEAK-BURST	(Optional) Specifies the burst size for the second token bucket in kilobytes.
confirm-action	(Optional) Specifies the action to take on green color packets. If not specified, the default action is **transmit**.
exceed-action	Specifies the action to take on packets that exceed the rate limit. For two rate policer, if not specified, the default action is **drop**.
violation-action	(Optional) Specifies the action to take on packets that violate the normal and maximum burst sizes for singe rate policing. Specifies the action to take for those packets that did not conform to both CIR and PIR. For a single rate policer, If violation-action is not specified, it will create a single rate two color policer. For a two rate policer, if not specified, the default action is the same as **exceed-action**.
ACTION	Specifies the action to take on packets. Specify one of the following keywords: **drop** - Drops the packet. **set-dscp-transmit** *VALUE* - Sets the IP DSCP value and transmits the packet with the new IP DSCP value. **set-1p-transmit** - Sets the 802.1p value and transmits the packet with the new value. **transmit** - Transmits the packet unaltered.
color-aware	(Optional) Specifies the option for the single rate three colors policer or two rates three colors policer. When color-aware is not specified, the policer works in the color blind mode. When color-aware is specified, the policer works in color aware mode.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

An aggregate policer can be shared by different policy map classes in a policy map. It cannot be shared by separate policy maps.

Example

This example shows how an aggregate policer named “agg-policer5” with a single rate two color policer is configured. This named aggregator policer is applied as the service policy for the class 1 and class 2 traffic class in the policy 2 policy map.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# mls qos aggregate-policer agg-policer5 10 1000 exceed-action
drop
GA-MLxxTPoE+(config)# policy-map policy2
GA-MLxxTPoE+(config-pmap)# class class1
GA-MLxxTPoE+(config-pmap-c)# police aggregate agg_policer5
GA-MLxxTPoE+(config-pmap-c)# exit
GA-MLxxTPoE+(config-pmap)# class class2
GA-MLxxTPoE+(config-pmap-c)# police aggregate agg_policer5
GA-MLxxTPoE+(config-pmap-c)#
```

5.2.5 mls qos cos

This command is used to configure the default Class of Service (CoS) value of a port. Use the **no** form of this command to revert to the default setting.

Syntax

- **mls qos cos** {*COS-VALUE* | **override**}
- **no mls qos cos**

Parameters

Parameters	Description
COS-VALUE	Specifies to assign a default CoS value to a port. This CoS will be applied to the incoming untagged packets received by the port.
override	Specifies to override the CoS of the packets. The default CoS will be applied to all incoming packets, tagged or untagged, received by the port.

Default

By default, this CoS value is 0.
By default, **override** is not specified.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

When the **override** option is not specified, the CoS of the packets will be the packet's CoS if the packets are tagged, and will be the port default CoS if the packet is untagged.
If the **override** option is specified, the port default CoS is applied to all packets received by the port. Use the **override** keyword when all incoming packets on certain ports deserve a higher or lower priority than packets that enter from other ports. Even if a port was previously set to trust DSCP or CoS, this command overrides that trust state, and all CoS values on the incoming packets are changed to the default CoS value that is configured with the **mls qos cos** command. If an incoming packet is tagged, the CoS value of the packet is modified at the ingress port.
For packets arriving at the 802.1Q VLAN tunnel port, the port default CoS will be both the internal CoS assigned to the packet, and the CoS value in the tunnel VLAN tag of the transmitted packet.

Example

This example shows how the default CoS of GigabitEthernet1/0/1 is set to 3.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface  gi1/0/1
GA-MLxxTPoE+(config-if)# mls qos cos 3
GA-MLxxTPoE+(config-if)#
```

5.2.6 mls qos dscp-mutation

This command is used to attach an ingress Differentiated Services Code Point (DSCP) mutation map to the interface. Use the no form of this command to remove the ingress DSCP mutation map association from the interface.

Syntax

- **mls qos dscp-mutation** *DSCP-MUTATION-TABLE-NAME*
- **no mls qos dscp-mutation**

Parameters

Parameters	Description
DSCP-MUTATION-TABLE-NAME	Specifies the name of the DSCP mutation table. The string of the name is up to 32 characters and no space is allowed.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use this command to attach an ingress DSCP mutation table to an interface. The ingress DSCP mutation will mutate the DSCP value right after the packet is received by the interface, and QoS handles the packet with this new value. The Switch sends the packet out the port with the new DSCP value.

Example

This example shows how to map DSCP 30 to the mutated DSCP value 8 and then attach the ingress-DSCP mutation map named “mutemap1” to GigabitEthernet1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# mls qos map dscp-mutation mutemap1 30 to 8
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# mls qos dscp-mutation mutemap1
GA-MLxxTPoE+(config-if)#
```

5.2.7 mls qos map cos-color

This command is used to define the CoS to color map for mapping a packet’s initial color. Use the **no** form of this command to revert to the default setting.

Syntax

- **mls qos map cos-color** *COS-LIST* **to {green | yellow | red}**
- **no mls qos map cos-color**

Parameters

Parameters	Description
COS-LIST	Specifies the list of CoS values to be mapped to a color. The range of CoS is from 0 to 7. The multiple CoS values in the list can be in the form separated by commas or a range list.
green	Specifies to be mapped to green.
yellow	Specifies to be mapped to yellow.
red	Specifies to be mapped to red.

Default

By default, all CoS values are mapped to the green color.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

When packets enter the ingress port, they will be colored based on either the DSCP to color map (if the port is a trusted DSCP port) or the CoS to color map (if the port is a trusted CoS port).
Use the **mls qos map cos-color** command, in the interface configuration mode, to configure the CoS to color map. If the ingress port is set to trusted CoS ports, the received packet will be initialized to a color based on this map.

Example

This example shows how to define CoS value 1 to 7 as the red color and 0 as the green color for packets arriving at GigabitEthernet1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# mls qos map cos-color 1-7 to red
GA-MLxxTPoE+(config-if)#
```

5.2.8 mls qos map dscp-color

This command is used to define the DSCP to color map for the mapping of a packet's initial color. Use the **no** form of this command to revert to the default setting.

Syntax

- **mls qos map dscp-color** *DSCP-LIST* **to {green | yellow | red}**
- **no mls qos map dscp-color** *DSCP-LIST*

Parameters

Parameters	Description
dscp *DSCP-LIST*	Specifies the list of DSCP code point to be mapped to a color. The range is from 0 to 63. The multiple DSCP values in the list can be in the form separated by commas or a range list.
green	Specifies to be mapped to green.
yellow	Specifies to be mapped to yellow.
red	Specifies to be mapped to red.

Default

There is no mapping. All DSCP code points are mapped to green color.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

This command is used to define the DSCP to color map for the mapping of a packet's initial color.

Example

This example shows how to define DSCP 61 to 63 as the yellow color and any other IP packet is initialized with the green color at GigabitEthernet1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# mls qos map dscp-color 61-63 to yellow
GA-MLxxTPoE+(config-if)#
```

5.2.9 mls qos map dscp-cos

This command is used to define a DSCP-to-CoS map. Use the **no** form of this command to revert to the default setting.

Syntax

- **mls qos map dscp-cos** *DSCP-LIST* **to** *COS-VALUE*
- **no mls qos map dscp-cos** *DSCP-LIST*

Parameters

Parameters	Description
dscp-cos *DSCP-LIST* **to** *COST-VALUE*	Specifies the list of DSCP code points to be mapped to a CoS value. The range is from 0 to 63. The series of DSCPs can be separated by commas (,) or hyphens (-) with no spaces or hyphens before and after.
DSCP-LIST	Specifies the range of DSCP values.

Default

CoS Value:	0	1	2	3	4	5	6	7
DSCP Value:	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

The DSCP to CoS map is used by a DSCP trust port to map a DSCP value to an internal CoS value. In turn this CoS value is then mapped to the CoS queue based on the CoS to queue map configured by the **priority-queue cos-map** command.

Example

This example shows how to configure the DSCP to CoS map for mapping DSCP 12, 16, and 18 to CoS 1 for GigabitEthernet1/0/6.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/6
GA-MLxxTPoE+(config-if)# mls qos map dscp-cos 12,16,18 to 1
GA-MLxxTPoE+(config-if)#
```

5.2.10 mls qos map dscp-mutation

This command is used to define a named DSCP mutation map. Use the **no** form of this command to remove the mutation map.

Syntax

- **mls qos map dscp-mutation** *MAP-NAME INPUT-DSCP-LIST* **to** *OUTPUT-DSCP*
- **no mls qos map dscp-mutation** *MAP-NAME*

Parameters

Parameters	Description
MAP-NAME	Specifies the name of the DSCP mutation map in a string length up to 32 characters (no space is allowed).

Parameters	Description
INPUT-DSCP-LIST	Specifies the list of DSCP code point to be mutated to another DSCP value. The range is from 0 to 63. A series of DSCPs can be separated by commas (,) or hyphens (-). No space or hyphen is before and after.
OUTPUT-DSCP	Specifies the mutated DSCP value. The value is from 0 to 63.

Default

The output DSCP is equal to the input DSCP.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

When a packet is received by an interface, based on a DSCP mutation map, the incoming DSCP can be mutated to another DSCP immediately before any QoS operations. The DSCP mutation is helpful to integrate domains with different DSCP assignments.
When configuring a named DSCP mutation map, note the following:

- Enter multiple commands to map additional DSCP values to a mutated DSCP value.
- Enter a separate command for each mutated DSCP value.

The DSCP-CoS map and DSCP-color map will still be based on the packet's original DSCP. All the subsequent operations will base on the mutated DSCP.

Example

This example shows how to map DSCP 30 to the mutated DSCP value 8, DSCP 20 to the mutated DSCP 10, with the mutation map named "mutemap1".

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# mls qos map dscp-mutation mutemap1 30 to 8
GA-MLxxTPoE+(config)# mls qos map dscp-mutation mutemap1 20 to 10
GA-MLxxTPoE+(config)#
```

5.2.11 mls qos scheduler

This command is used to configure the scheduling mechanism. Use the **no** form of this command to revert to the default setting.

Syntax

- **mls qos scheduler {sp | rr | wrr | wdrr}**
- **no mls qos scheduler**

Parameters

Parameters	Description
sp	Specifies that all queues are in strict priority scheduling.
rr	Specifies that all queues are in round-robin scheduling.
wrr	Specifies the queues in the frame count weighted round-robin scheduling. If the weight of a queue be configured to zero, the queue is in the SP scheduling mode.
wdrr	Specifies the queues of all ports in the frame length (quantum) weighted deficit round-robin scheduling. If the weight of a queue be configured to zero, the queue is in the SP scheduling mode.

Default

The default queue scheduling algorithm is WRR.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Specify schedule algorithms to WRR, SP, RR or WDRR for the output queue. By default, the output queue scheduling algorithm is WRR. WDRR operates by serving an accumulated set of backlogged credits in the transmit queue in a round robin order. Initially, each queue sets its credit counter to a configurable quantum value. Every time a packet from a CoS queue is sent, the size of the packet is subtracted from the corresponding credit counter and the service right

is turned over to the next lower CoS queue. When the credit counter drops below 0, the queue is no longer serviced until its credits are replenished. When the credit counters of all CoS queues reaches 0, the credit counters will be replenished at that time.
All packets are serviced until their credit counter is zero or negative and the last packet is transmitted completely. When this condition happens, the credits are replenished. When the credits are replenished, a quantum of credits are added to each CoS queue credit counter. The quantum for each CoS queue may be different based on the user configuration.
To set a CoS queue in the strict priority mode, any higher priority CoS queue must also be in the strict priority mode.
WRR operates by transmitting permitted packets into the transmit queue in a round robin order. Initially, each queue sets its weight to a configurable weighting. Every time a packet from a higher priority CoS queue is sent, the corresponding weight is subtracted by 1, and the packet in the next lower CoS queue will be serviced. When the weight of a CoS queue reaches zero, the queue will not be serviced until its weight is replenished. When weights of all CoS queues reach 0, the weights get replenished at a time.

Example

This example shows how to configure the queue scheduling algorithm to the strict priority mode.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# mls qos scheduler sp
GA-MLxxTPoE+(config-if)#
```

5.2.12 mls qos trust

This command is used to configure the trust state of a port to trust either the CoS field or the DSCP field of the arriving packet for subsequent QoS operation. Use the **no** form of this command to revert to the default setting.

Syntax

- **mls qos trust {cos | dscp}**
- **no mls qos trust**

Parameters

Parameters	Description
cos	Specifies that the CoS bits of the arriving packets are trusted for subsequent QoS operations.
dscp	Specifies that the ToS/DSCP bits, if available in the arriving packets, are trusted for subsequent operations. For non-IP packet, Layer 2 CoS information will be trusted for traffic classification.

Default

By default, CoS is trusted.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

When the interface is set to trust DSCP, the DSCP of the arriving packet will be trusted for the subsequent QoS operations. First, the DSCP will be mapped to an internal CoS value, which will be subsequently used to determine the CoS queue. The DSCP to CoS map is configured by the **mls qos map dscp-cos** command. The CoS to queue map is configured by the **priority-queue cos-map** command. If the arriving packet is a non-IP packet, the CoS is trusted. The resulting CoS mapped from DSCP will also be the CoS in the transmitted packet.
When an interface is in the trust CoS state, the CoS of the arriving packet will be applied to the packet as the internal CoS and used to determine the CoS queue. The CoS queue is determined based on the CoS to Queue mapping table.
When a packet arrives at an 802.1Q VLAN tunnel port, the packet will be added with an outer VLAN tag in order to transmit through the VLAN tunnel. If the port is to trust CoS, then the inner tag CoS will be the internal CoS of the packet and the CoS value in the packet's outer VLAN tag. If the MLS QoS CoS override is configured, then the CoS specified by command **mls qos cos** will be the internal CoS of the packet and the CoS value in the packet's outer VLAN tag. If the port is to trust DSCP, then the CoS mapped from the DSCP code point will be the internal CoS of the packet and the CoS value in the packet's outer VLAN tag

When a packet is received by a port, it will be initialized to a color based on the **mls qos map dscp-color** command if the receiving port is to trust DSCP or MLS QoS mapped CoS color if the receiving port is to trust CoS.

Example

This example shows how to configure GigabitEthernet1/0/1 to trust the DSCP mode.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# mls qos trust dscp
GA-MLxxTPoE+(config-if)#
```

5.2.13 police

This command is used to configure traffic policing to use the single rate. Use the **no** form of this command to remove traffic policing.

Syntax

- **police** *KBPS* [*BURST-NORMAL* [*BURST-MAX*]] [**conform-action** *ACTION*] **exceed-action** *ACTION* [**violate-action** *ACTION*] [**color-aware**]
- **no police**

Parameters

Parameters	Description
KBPS	Specifies the average rate, in kilobits per second.
BURST-NORMAL	(Optional) Specifies the normal burst size in kilobytes.
BURST-MAX	(Optional) Specifies the maximum burst size, in kilobytes.
confirm-action	(optional) Specifies the action to take on green color packets. If the action is not specified, the default action is to transmit.
exceed-action	Specifies the action to take on yellow color packets that exceed the rate limit.
violate-action	(Optional) Specifies the action to take on red color packets. When violate-action is not specified, the policer is a single rate two color policer. When violate-action is specified, the policer is a single rate three color policer.

Parameters	Description
ACTION	Specifies the action to take on packets. Use one of the following keywords: **drop** - Drops the packet. **set-dscp-transmit** *VALUE* - Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value. **set-1p-transmit** - Sets the 802.1p value and transmits the packet with the new value. **transmit** - Transmits the packet. The packet is not altered.
color-aware	(Optional) Specifies the option for the single rate three colors policer. When color-aware is not specified, the policer works in the color blind mode. When color-aware is specified, the policer works in the color aware mode.

Default

None

Command Mode

Policy-map Class Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use the **police** command to drop the packet or mark the packet with different quality of service (QoS) values based on conformance level of the packet.
Use the **police** *KBPS* command to create a single rate policer. Use the **police cir** command to create a two rate policer. There are two kinds of single rate policers (1) a single rate two color policer and (2) a single rate three color policer. If the violate action is specified in the **police** *KBPS* command, then the policer is three colors. If not specified, the policer is two colors.
As a packet arrives at a port, the packet will be initialized with a color. If the receive port trusts DSCP then the initial color of the packet is mapped from the incoming DSCP based on the DSCP to color map. If the receipt port trusts CoS then the initial color is mapped from the incoming CoS based on the CoS to color map.

A single rate two color policer can only work in color-blind mode. Both single rate three color policers and two rate three color policers can work in color aware mode. In color-blind mode, the final color of the packet is determined by the policer metering result alone. In color-aware mode, the final color of the packet is determined by the initial color of the packet and the policer metering result. In this case the policer may further downgrade the initial color.
After the policer metering action will be based on the final color. Conform action will be taken on green color packets, exceed-action will be taken on yellow color packets, and violate action will be taken on red color packets. When specifying actions, you cannot specify contradictory actions such as violate-action transmit and exceed-action drop.
The actions configured by the set command for a traffic class will be applied to all the packets belonging to the traffic class.

Example

This example shows how to define a traffic class and associate the policy with the match criteria for the traffic class in a policy map. The **service-policy** command is then used to attach this service policy to the interface. In this particular example, traffic policing is configured with an average rate of 8 kilobits per second and a normal burst size of 1 kilobyte for all ingress packets at GigabitEthernet1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# class-map access-match
GA-MLxxTPoE+(config-cmap)# match access-group name acl_rd
GA-MLxxTPoE+(config-cmap)# exit
GA-MLxxTPoE+(config)# policy-map police-setting
GA-MLxxTPoE+(config-pmap)# class access-match
GA-MLxxTPoE+(config-pmap-c)# police 8 1 exceed-action drop
GA-MLxxTPoE+(config-pmap-c)# exit
GA-MLxxTPoE+(config-pmap)# exit
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# service-policy input police-setting
GA-MLxxTPoE+(config-if)#
```

5.2.14 police aggregate

This command is used to configure a named aggregate policer as the policy for a traffic class in a policy map. Use the **no** form of this command to delete the name aggregate policer from a class policy.

Syntax

- **police aggregate** *NAME*
- **no police**

Parameters

Parameters	Description
NAME	Specifies a previously defined aggregate policer name as the aggregate policer for a traffic class.

Default

None

Command Mode

Policy-map Class Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use the **mls qos aggregate-policer** command in the global configuration mode to create a named aggregate policer. Then use the **police aggregate** command in the policy-map class configuration mode to configure the named aggregate policer as the policy for a traffic class. A named aggregate policer cannot be referenced from a different policy map. If a named aggregate policer is attached to multiple ingress ports, the metering operation of the policer will not be applied to the aggregate traffic but remains applied to the traffic received on the individual port.

Example

This example shows how to configure a named aggregate policer's parameters and apply the policer to multiple classes in a policy map: An aggregate policer with single rate policing named "agg_policer1" is created. This policer is configured as the policy for traffic class 1, 2, and 3.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# mls qos aggregate-policer agg_policer1 10000 16384 exceed-
action drop
GA-MLxxTPoE+(config)# policy-map policy2
GA-MLxxTPoE+(config-pmap)# class class1
GA-MLxxTPoE+(config-pmap-c)# police aggregate agg_policer1
GA-MLxxTPoE+(config-pmap-c)# exit
GA-MLxxTPoE+(config-pmap)# class class2
GA-MLxxTPoE+(config-pmap-c)# police aggregate agg_policer1
GA-MLxxTPoE+(config-pmap-c)# exit
GA-MLxxTPoE+(config-pmap)# class class3
GA-MLxxTPoE+(config-pmap-c)# police aggregate agg_policer1
GA-MLxxTPoE+(config-pmap-c)#
```

5.2.15 police cir

This command is used to configure traffic policing for two rates, the CIR and the PIR. Use the **no** form of this command to remove two-rate traffic policing.

Syntax

- **police cir** *CIR* [**bc** *CONFORM-BURST*] **pir** *PIR* [**be** *PEAK-BURST*] [**conform-action** *ACTION*] [**exceed-action** *ACTION* [**violate-action** *ACTION*]] [**color-aware**]
- **no police**

Parameters

Parameters	Description
CIR	Specifies the committed information rate in kilobits per second. The committed packet rate is the first token bucket for the two-rate metering.
PIR	Specifies the peak information rate in kilobits per second. The peak information rate is the second token bucket for the two-rate metering.
CONFORM-BURST	(Optional) Specifies the burst size for the first token bucket in kilobytes.
PEAK-BURST	(Optional) Specifies the burst size for the second token bucket in kilobytes.
confirm-action	(Optional) Specifies the action to take on green color packets. If not specified, the default action is **transmit**.

Parameters	Description
exceed-action	(Optional) Specifies the action to take for those packets that conform to PIR but not to CIR. These packets are referred to as yellow color traffic. If not specified, the default action is **drop**.
violate-action	(Optional) Specifies the action to take for those packets that did not conform to both CIR and PIR. These packets are referred to as red color traffic. If not specified, the default action is the same as **exceed-action**.
ACTION	(Optional) Specifies the action to be taken. The actions can be: **drop** - Packets will be dropped. **set-dscp-transmit** *VALUE* - Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value. **set-1p-transmit** - Sets the 802.1p value and transmits the packet with the new value. **transmit** - Transmits the packet. The packet is not altered.
color-aware	(Optional) Specifies the option for a two rate three color policer. When color-aware is not specified, the policer works in the color blind mode. When color-aware is specified, the policer works in the color aware mode.

Default

None

Command Mode

Policy-map Class Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

As a packet arrives at a port, the packet will be initialized with a color. The receiving port either trusts DSCP or CoS. The initial color of the packet is mapped from the DSCP in the incoming packet if the receiving port trusts DSCP. The initial color of the packet is mapped from the CoS in the incoming packet if the receiving port trusts CoS.

Both single rate three colors policers and two rate three color policers can work in color aware mode. In color-blind mode, the final color of the packet is determined by the policer metering result alone. In color-aware mode, the final color of the packet is determined by the initial color of the packet, and the policer metering result. The policer may further downgrade the initial color.
After the policer metering, and based on the final color, **conform-action** will be taken on green color packets, **exceed-action** will be taken on yellow color packets, and **violate-action** will be taken on red color packets. When specifying the actions, you cannot specify contradictory actions such as **violate-action transmit** and **exceed-action drop**.
The actions configured by the set command for the traffic class will be applied to all the packets belonging to the traffic class.

Example

This example shows how two-rate traffic policing is configured on a class called police to limit traffic to an average committed rate of 500 kbps and a peak rate of 1 Mbps, and the policy map named policy1 is attached to gi1/0/3.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# class-map police
GA-MLxxTPoE+(config-cmap)# match access-group name myAcl101
GA-MLxxTPoE+(config-cmap)# exit
GA-MLxxTPoE+(config)# policy-map policy1
GA-MLxxTPoE+(config-pmap)# class police
GA-MLxxTPoE+(config-pmap-c)# police cir 500 bc 10 pir 1000 be 10 exceed-action set-dscp-transmit 2 violate-action drop
GA-MLxxTPoE+(config-pmap-c)# exit
GA-MLxxTPoE+(config-pmap)# exit
GA-MLxxTPoE+(config)# interface gi1/0/3
GA-MLxxTPoE+(config-if)# service-policy output policy1
GA-MLxxTPoE+(config-if)#
```

5.2.16 policy-map

This command is used to enter the policy-map configuration mode and create or modify a policy map that can be attached to one or more interfaces as a service policy. Use the **no** form of this command to delete a policy map.

Syntax

- **policy-map** *NAME*
- **no policy-map** *NAME*

Parameters

Parameters	Description
NAME	Specifies the name of the policy map. The name can be a maximum of 32 alphanumeric characters.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use the **policy-map** command to enter the policy-map configuration mode from where the user can configure or modify the policy for the traffic class. A single policy map can be attached to more than one interface concurrently. The succeeding policy-map attaches overwrite the previous one.
Policy maps contain traffic classes. Traffic classes contain one or more match commands that can be used to match packets (and organize them into groups) on the basis of a protocol type or application.

Example

This example shows how to create a policy map called policy and configures two class policies within the policy map. The class policy called class1 specifies a policy for traffic that matches an access control list (ACL) “acl_rd”. The second class is the default class, named class-default to include packets that do not match the defined classes.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# class-map class1
GA-MLxxTPoE+(config-cmap)# match access-group name acl_rd
GA-MLxxTPoE+(config-cmap)# exit
GA-MLxxTPoE+(config)# policy-map policy
GA-MLxxTPoE+(config-pmap)# class class1
GA-MLxxTPoE+(config-pmap-c)# set ip dscp 46
GA-MLxxTPoE+(config-pmap-c)# exit
GA-MLxxTPoE+(config-pmap)# class class-default
GA-MLxxTPoE+(config-pmap-c)# set ip dscp 00
GA-MLxxTPoE+(config-pmap-c)#
```

5.2.17 priority-queue cos-map

This command is used to define a Class of Service (CoS) to queue map. Use the **no** form of this command to revert to the default setting.

Syntax

- **priority-queue cos-map** *QUEUE-ID COS1* [*COS2* [*COS3* [*COS4* [*COS5* [*COS6* [*COS7* [*COS8*]]]]]]]
- **no priority-queue cos-map**

Parameters

Parameters	Description
QUEUE-ID	Specifies the queue ID the CoS will be mapped.
COS1	Specifies the mapping CoS value. Valid values are from 0 to 7.
COS2…COS8	(Optional) Specifies the mapping CoS value. Valid values are from 0 to 7.

Default

The default priority (CoS) to queue mapping is: 0 to 2, 1 to 0, 2 to 1, 3 to 3, 4 to 4, 5 to 5, 6 to 6, 7 to 7.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

When a packet is received, the packet will be given an internal CoS. This internal CoS is used to select the transmit queue based on the CoS to queue map. The CoS queue with a higher number will receive a higher priority.

Example

This example shows how to assign CoS priority 3, 5 and 6 to queue 2.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# priority-queue cos-map 2 3 5 6
GA-MLxxTPoE+(config)#
```

5.2.18 queue rate-limit

This command is used to specify or modify the bandwidth allocated for a queue. Use the **no** form of this command to remove the bandwidth allocated for a queue.

Syntax

- **queue** *QUEUE-ID* **rate-limit** {*MIN-BANDWIDTH-KBPS* | **percent** *MIN-PERCENTAGE*} {*MAX-BANDWIDTH-KBPS* | **percent** *MAX-PERCENTAGE*}
- **no queue** *QUEUE-ID* **rate-limit**

Parameters

Parameters	Description
QUEUE-ID	Specifies the queue ID to set minimal guaranteed and maximum bandwidth.
MIN-BANDWIDTH-KBPS	Specifies the minimal guaranteed bandwidth in kilobits per second allocated to a specified queue.
MAX-BANDWIDTH-KBPS	Specifies the maximum bandwidth in kilobits per second for a specified queue.
MIN-PERCENTAGE	Specifies to set the minimal bandwidth by percentage. The valid range is from 1 to 100.
MAX-PERCENTAGE	Specifies to set the maximum bandwidth by percentage. The valid range is from 1 to 100.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use this command to configure the minimal and maximum bandwidth for a specified queue. When the minimal bandwidth is configured, the packet transmitted from the queue can be guaranteed. When the maximum bandwidth is configured, packets transmitted from the queue cannot exceed the maximum bandwidth even if the bandwidth is available.
When configuring the minimal bandwidth, the aggregate of the configured minimum bandwidth must be less than 75 percent of the interface bandwidth to make sure the configured minimal bandwidth can be guaranteed. It is not necessary to set the minimum guaranteed bandwidth for the highest strict priority queue. This is because the traffic in this queue will be serviced first if the minimal bandwidth of all queues is satisfied.
The configuration of this command can only be attached to a physical port but not a port-channel. That is the minimum guaranteed bandwidth of one CoS cannot be used across physical ports.

Example

This example shows how to configure the queue bandwidth, the minimum guaranteed bandwidth and maximum bandwidth of queue 1 of GigabitEthernet1/0/1 to 100Kbps and 2000Kbps respectively. Set the minimum guaranteed bandwidth and maximum bandwidth of queue 2 to 10% and 50% respectively.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# queue 1 rate-limit 100 2000
GA-MLxxTPoE+(config-if)# queue 2 rate-limit percent 10 percent 50
GA-MLxxTPoE+(config-if)#
```

5.2.19 rate-limit {input | output}

This command is used to set the received or transmitted bandwidth limit values for an interface. Use the **no** form of this command to disable the bandwidth limit.

Syntax

- **rate-limit** {**input** | **output**} {*NUMBER-KBPS* | **percent** *PERCENTAGE*} [*BURST-SIZE*]
- **no rate-limit** {**input** | **output**}

Parameters

Parameters	Description
input	Specifies the bandwidth limit for ingress packets.
output	Specifies the bandwidth limit for egress packets.
NUMBER-KBPS	Specifies the number of kilobits per second as the maximum bandwidth limit.
PERCENTAGE	Specifies to set the limited rate by percentage. The valid range is 1 to 100.
BURST-SIZE	(Optional) Specifies the limit for burst traffic in Kbyte.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

The specified limitation cannot exceed the maximum speed of the specified interface. For the ingress bandwidth limitation, the ingress will send a pause frame or a flow control frame when the received traffic exceeds the limitation.

Example

This example shows how the maximum bandwidth limits are configured on GigabitEthernet1/0/5. The ingress bandwidth is limited to 2000Kbps and 4096K bytes for burst traffic.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/5
GA-MLxxTPoE+(config-if)# rate-limit input 2000 4096
GA-MLxxTPoE+(config-if)#
```

5.2.20 service-policy

This command is used to attach a policy map to the input or output type on an interface. Use the **no** form of this command to remove a service policy from an input interface.

Syntax

- service-policy {input | output} *NAME*
- no service-policy {input | output}

Parameters

Parameters	Description
input	Specifies to apply the policy map for ingress flow on the interface.
output	Specifies to apply the policy map for egress flow on the interface.
NAME	Specifies the name of a service policy map. The name can be a maximum of 32 alphanumeric characters.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use this command to attach at most one policy map for each type (input or output) on an interface. This policy is attached to the interface for aggregate and controls the number or rate of packets. A packet arriving at a port will be treated based on the service policy attached to the interface.

Example

This example shows how two policy maps are defined: (1) cust1-classes and (2) cust2-classes.
For cust1-classes, gold is configured to match CoS 6 and be policed by a single rate policer with a committed rate of 800 Kbps. Silver is configured to match CoS 5 and be policed by a single rate policer with a committed rate of 2000Kbps, and bronze is configured to match CoS 0 and be policed by a single rate policer with a committed rate of 8000Kbps.

For cust2-classes, gold is configured to use Cos Queue 6 and be policed by a single rate policer with a committed rate of 1600 Kbps. Silver is policed by a single rate policer with a committed rate of 4000 Kbps, and bronze is policed by a single rate policer with a committed rate of 16000 Kbps.
The cust1-classes policy map is configured and then attached to interfaces GigabitEthernet1/0/1 and 1/0/2 for ingress traffic.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# class-map match-all gold
GA-MLxxTPoE+(config-cmap)# match cos 6
GA-MLxxTPoE+(config-cmap)# exit
GA-MLxxTPoE+(config)# class-map match-all silver
GA-MLxxTPoE+(config-cmap)# match cos 5
GA-MLxxTPoE+(config-cmap)# exit
GA-MLxxTPoE+(config)# class-map match-all bronze
GA-MLxxTPoE+(config-cmap)# match cos 0
GA-MLxxTPoE+(config-cmap)# exit
GA-MLxxTPoE+(config)# policy-map cust1-classes
GA-MLxxTPoE+(config-pmap)# class gold
GA-MLxxTPoE+(config-pmap-c)# police 800 2000 exceed-action set-dscp-transmit 0
GA-MLxxTPoE+(config-pmap-c)# exit
GA-MLxxTPoE+(config-pmap)# class silver
GA-MLxxTPoE+(config-pmap-c)# police 2000 2000 exceed-action set-dscp-transmit 0
GA-MLxxTPoE+(config-pmap-c)# exit
GA-MLxxTPoE+(config-pmap)# class bronze
GA-MLxxTPoE+(config-pmap-c)# police 8000 2000 exceed-action set-dscp-transmit 0
GA-MLxxTPoE+(config-pmap-c)# exit
GA-MLxxTPoE+(config-pmap)# exit
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# service-policy input cust1-classes
GA-MLxxTPoE+(config-if)# exit
GA-MLxxTPoE+(config)# interface gi1/0/2
GA-MLxxTPoE+(config-if)# service-policy input cust1-classes
GA-MLxxTPoE+(config-if)#
```

The cust2-classes policy map is configured and then attached to interface GigabitEthernet1/0/1 for ingress traffic.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# policy-map cust2-classes
GA-MLxxTPoE+(config-pmap)# class gold
GA-MLxxTPoE+(config-pmap-c)# police 1600 2000 exceed-action set-dscp-transmit 0
GA-MLxxTPoE+(config-pmap-c)# exit
GA-MLxxTPoE+(config-pmap)# class silver
GA-MLxxTPoE+(config-pmap-c)# police 4000 2000 exceed-action set-dscp-transmit 0
GA-MLxxTPoE+(config-pmap-c)# exit
GA-MLxxTPoE+(config-pmap)# class bronze
GA-MLxxTPoE+(config-pmap-c)# police 16000 2000 exceed-action set-dscp-transmit 0
GA-MLxxTPoE+(config-pmap-c)# exit
GA-MLxxTPoE+(config-pmap)# exit
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# service-policy input cust2-classes
GA-MLxxTPoE+(config-if)#
```

5.2.21 set

This command is used to configure the new precedence field, DSCP field, and CoS field of the outgoing packet. The user can also specify the CoS queue for the packet.

Syntax

- **set** {[**ip**] **precedence** *PRECEDENCE* | [**ip**] **dscp** *DSCP* | **cos** *COS* | **cos-queue** *COS-QUEUE*}
- **no set** {[**ip**] **precedence** *PRECEDENCE* | [**ip**] **dscp** *DSCP* | **cos** *COS* | **cos-queue** *COS-QUEUE*}

Parameters

Parameters	Description
precedence *PRECEDENCE*	Specifies a new precedence for the packet. The range is from 0 to 7. If the optional keyword **ip** is specified, IPv4 precedence will be marked. If not specified, both IPv4 and IPv6 precedence will be marked. For IPv6 packets, the precedence is the most three significant bits of traffic class of IPv6 header.
dscp *DSCP*	Specifies a new DSCP for the packet. The range is from 0 to 63. If the optional keyword **ip** is specified, IPv4 DSCP will be marked. If not specified, both IPv4 and IPv6 DSCP will be marked.
cos *COS*	Specifies to assign a new CoS value to the packet. The range is from 0 to 7.
cos-queue *COS-QUEUE*	Specifies to assign the CoS queue to the packets. This overwrites the original CoS queue selection. Setting the CoS queue will not take effect if the policy map is applied for the egress flow on the interface.

Default

None

Command Mode

Policy-map Class Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use this command to set the DSCP field, CoS field, or precedence field of the matched packet to a new value. Use the **set cos-queue** command to directly assign the CoS queue to the matched packets.
Configure multiple set commands for a class if they are not conflicting.
The **set dscp** command will not affect the CoS queue selection. The **set cos-queue** command will not alter the CoS field of the outgoing packet. The user can use the **police** command and the **set** command for the same class. The **set** command will be applied to all colors of packets.

Example

This example shows how the policy map policy1 is configured with the policy for the class1 class. The packets that are included in the class1 class will be set to a DSCP of 10 and policed by a single rate policer with a committed rate of 1Mbps.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# policy-map policy1
GA-MLxxTPoE+(config-pmap)# class class1
GA-MLxxTPoE+(config-pmap-c)# set ip dscp 10
GA-MLxxTPoE+(config-pmap-c)# police 1000000 2000 exceed-action set-dscp-transmit 10
GA-MLxxTPoE+(config-pmap-c)# exit
GA-MLxxTPoE+(config-pmap)#
```

5.2.22 show class-map

This command is used to display the class map configuration.

Syntax

- **show class-map** [*NAME*]

Parameters

Parameters	Description
NAME	(Optional) Specifies the name of the class map. The class map name can be a maximum of 32 alphanumeric characters.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guidelines

Use this command to display all class maps and their matching criteria.

Example

This example shows how two class maps are defined. Packets that match the access list "acl_home_user" belong to the class "c3", IP packets belong to the class "c2".

```
GA-MLxxTPoE+# show class-map

Class Map match-any class-default
   Match any

Class Map match-all c2
   Match protocol ip

Class Map match-all c3
   Match access-group acl_home_user

GA-MLxxTPoE+#
```

5.2.23 show mls qos aggregate-policer

This command is used to display the configured aggregated policer.

Syntax

- **show mls qos aggregate-policer** [*NAME*]

Parameters

Parameters	Description
NAME	(Optional) Specifies the name of the aggregate policer.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guidelines

This command is used to display the configured aggregated policer.

Example

This example shows how to display the aggregate policer.

```
GA-MLxxTPoE+# show mls qos aggregate-policer

mls qos aggregate-policer agg-policer5 10 1000 conform-action transmit exceed-action
drop
mls qos aggregate-policer agg-policer5 cir 500 bc 10 pir 1000 be 10 conform-action
transmit exceed-action set-dscp-transmit 2 violate-action drop

GA-MLxxTPoE+#
```

5.2.24 show mls qos interface

This command is used to display port level QoS configurations.

Syntax

- **show mls qos interface** *INTERFACE-ID* [**,** | **-**] {**cos** | **scheduler** | **trust** | **rate-limit** | **queue-rate-limit** | **dscp-mutation** | **map** {**dscp-color** | **cos-color** | **dscp-cos**}}

Parameters

Parameters	Description
interface *INTERFACE-ID*	Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Parameters	Description
cos	Specifies to display the port default CoS.
scheduler	Specifies to display the transmit queue scheduling settings.
trust	Specifies to display the port trust State.
rate-limit	Specifies to display the bandwidth limitation configured for the port.
queue-rate-limit	Specifies to display the bandwidth allocation configured for the queue.
dscp-mutation	Specifies to display the DSCP mutation map attached to the interface.
map dscp-color	Specifies to display the DSCP to color map.
map cos-color	Specifies to display the CoS to color map.
map dscp-cos	Specifies to display the mapping of DSCP to CoS

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guidelines

This command is used to display port level QoS configurations.

Example

This example shows how to display the default CoS for eth 1/0/2 to eth 1/0/5.

```
GA-MLxxTPoE+# show mls qos interface gi1/0/2-5 cos

Interface  CoS   Override
---------- ----   ---------
Gi1/0/2      3      Yes
Gi1/0/3      4      No
Gi1/0/4      4      No
Gi1/0/5      3      No

GA-MLxxTPoE+#
```

This example shows how to display the port trust state for eth 1/0/2 to eth 1/0/5.

```
GA-MLxxTPoE+# show mls qos interface gi 1/0/2-1/0/5 trust

Interface   Trust State
---------- ------------
Gi1/0/2     trust DSCP
Gi1/0/3     trust CoS
Gi1/0/4     trust DSCP
Gi1/0/5     trust CoS

GA-MLxxTPoE+#
```

This example shows how to display the scheduling configuration for gi1/0/1 to 1/0/2.

```
GA-MLxxTPoE+# show mls qos interface gi 1/0/1-1/0/2 scheduler

Interface   Scheduler Method
----------  ------------------
Gi1/0/1      sp
Gi1/0/2      wrr

GA-MLxxTPoE+#
```

This example shows how to display the DSCP mutation maps attached to eth 1/0/1 to 1/0/2.

```
GA-MLxxTPoE+# show mls qos interface gi 1/0/1-2 dscp-mutation

Interface   DSCP Mutation Map
----------  ------------------
Gi1/0/1       Mutate Map 1
Gi1/0/2       Mutate Map 2

GA-MLxxTPoE+#
```

This example shows how to display the bandwidth allocation for port 1/0/1 to 1/0/4.

```
GA-MLxxTPoE+# show mls qos interface gi 1/0/1-4 rate-limit

Interface    Rx Rate              Tx Rate             Rx Burst   Tx Burst
----------  ------------------    -----------------   ---------  --------
Gi1/0/1    1000 kbps             No Limit            64 kbyte   No Limit
Gi1/0/2    No Limit              2000 kbps           No Limit   2000 kbyte
Gi1/0/3    10%(100000 kbps)      20%(200000 kbps)    64 kbyte   64 kbyte
Gi1/0/4    2%                    2000 kbps           64 kbyte   64 kbyte

GA-MLxxTPoE+#
```

This example shows how to display the CoS bandwidth allocation for eth 1/0/1 to 1/0/2.

```
GA-MLxxTPoE+# show mls qos interface gi 1/0/1-2 queue-rate-limit

Gi1/0/1
  QID   Min Bandwidth  Max Bandwidth
  ----  -------------- -------------
  0         -               -
  1         16 kbps         10%(100000 kbps)
  2         32 kbps             -
  3         2%              50%
  4         64 kbps             -
  5         64 kbps             -
  6         32 kbps             -
  7         -               128 kbps
Gi1/0/2
  QID   Min Bandwidth  Max Bandwidth
   ----  -------------- -------------
  0         -               -
  1         16 kbps             -
  2         32 kbps             -
  3         32 kbps             -
  4         64 kbps             -
  5         64 kbps             -
  6         32 kbps             -
  7         -               128 kbps

GA-MLxxTPoE+#
```

This example shows how to display the DSCP to color map for port 1/0/1 to port 1/0/2.

```
GA-MLxxTPoE+# show mls qos interface gi 1/0/1-2 map dscp-color

Gi1/0/1
  DSCP 0-7 are mapped to green
  DSCP 8-40 are mapped to red
  DSCP 41-43 are mapped to yellow
Gi1/0/2
  DSCP 0 - 7 are mapped to green

GA-MLxxTPoE+#
```

This example shows how to display the CoS to color map for port 1/0/3 to port 1/0/4.

```
GA-MLxxTPoE+# show mls qos interface gi 1/0/3-4 map cos-color

Gi1/0/3
  CoS 0,1,2 are mapped to green
  CoS 3-4 are mapped to yellow
  CoS 6 are mapped to red
Gi1/0/4
  CoS 0,1-6 are mapped to green

GA-MLxxTPoE+#
```

This example shows how to display the DSCP to CoS map for port 1/0/1.

```
GA-MLxxTPoE+# show mls qos interface gi 1/0/1 map dscp-cos

Gi1/0/1
    0  1  2  3  4  5  6  7  8  9
  --------------------------------
00  00 00 00 00 00 00 00 00 01 01
10  01 01 01 01 01 01 02 02 02 02
20  02 02 02 02 03 03 03 03 03 01
30  03 03 04 04 04 04 04 04 04 04
40  05 05 05 05 05 05 05 05 06 06
50  06 06 06 06 06 06 07 07 07 07
60  07 07 07 07

GA-MLxxTPoE+#
```

5.2.25 show mls qos map dscp-mutation

This command is used to display the QoS DSCP mutation map configuration.

Syntax

- **show mls qos map dscp-mutation** [*MAP-NAME*]

Parameters

Parameters	Description
MAP-NAME	(Optional) Specifies the name of the DSCP mutation map to be displayed.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guidelines

This command is used to display the QoS DSCP mutation map configuration.

Example

This example shows how to display the global DSCP mutation map.

```
GA-MLxxTPoE+#show mls qos map dscp-mutation

DSCP Mutation: mutation
Attaching interface:
   Gi1/0/2-1/0/3,1/0/8-1/0/10

       0  1  2  3  4  5  6  7  8  9
     --------------------------------
   00  00 10 02 10 04 05 06 07 08 09
   10  10 11 12 13 14 15 16 17 18 19
   20  20 21 22 23 24 25 26 27 28 29
   30  30 31 32 33 34 35 36 37 38 39
   40  40 41 42 43 44 45 46 47 48 49
   50  50 51 52 53 54 55 56 57 58 59
   60  60 61 62 63


GA-MLxxTPoE+#
```

5.2.26 show mls qos queueing

This command is used to display the QoS queuing information and weight configuration for different scheduler algorithm on specified interface(s).

Syntax

- **show mls qos queuing [interface** *INTERFACE-ID* **[, | -]]**

Parameters

Parameters	Description
interface *INTERFACE-ID*	(Optional) Specifies the interface ID on which the weight configuration of different scheduler.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guidelines

When the optional keyword Interface is entered, the weight configuration for different scheduler (WRR or WDRR) on the specified interface(s) will be displayed. If the interface is not specified, only the system-wide map of CoS to queue ID is displayed.
The scheduling mode which is configured by the **mls qos scheduler** command determines which weight configuration taking effect. Use the **show mls qos interface scheduler** command to get the scheduling mode of an interface.

Example

This example shows how to display the QoS queuing information.

```
GA-MLxxTPoE+#show mls qos queueing

 CoS-queue map:
   CoS    QID
   ---    ---
    0      2
    1      0
    2      1
    3      3
    4      4
    5      5
    6      6
    7      7


GA-MLxxTPoE+#
```

This example shows how to display the weight configuration for the different scheduler on GigabitEthernet1/0/3.

```
GA-MLxxTPoE+#show mls qos queueing interface gi1/0/3

Interface: Gi1/0/3
 wrr bandwidth weights:
   QID  Weights
   ---  -------
    0      1
    1      1
    2      1
    3      1
    4      1
    5      1
    6      1
    7      0
 wdrr bandwidth weights:
   QID  Quantum
   ---  -------
    0      1
    1      1
    2      1
    3      1
    4      1
    5      1
    6      1
    7      1

GA-MLxxTPoE+#
```

5.2.27 show policy-map

This command is used to display the policy map configuration.

Syntax

- **show policy-map** [*POLICY-NAME* | **interface** *INTERFACE-ID*]

Parameters

Parameters	Description
POLICY-NAME	(Optional) Specifies the name of the policy map. If not specified, all policy maps will be displayed.
interface *INTERFACE-ID*	(Optional) Specifies the module and port number.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guidelines

The **show policy-map** command displays the class policies configured for the policy map. Use the **show policy-map** command to display the class policy configurations of any or all the existing service policy maps.

Example

This example shows how in the policy map called policy1, two-rate traffic policing has been configured for the class called police. Two-rate traffic policing has been configured to limit the traffic to an average committed rate of 500 kbps and a peak rate of 1 Mbps.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# class-map police
GA-MLxxTPoE+(config-cmap)# match access-group name acl_rd
GA-MLxxTPoE+(config-cmap)#exit
GA-MLxxTPoE+(config)#policy-map policy1
GA-MLxxTPoE+(config-pmap)# class police
GA-MLxxTPoE+(config-pmap-c)# police cir 500 bc 10 pir 1000 be 10 exceed-action set-dscp-transmit 2 violate-action drop
GA-MLxxTPoE+(config-pmap-c)# exit
GA-MLxxTPoE+(config-pmap)# exit
GA-MLxxTPoE+(config)# interface gi1/0/1
Router(config-if)# service-policy output policy1
Router(config-if)#
```

This example shows how to the display of the policy map called policy1, created above.

```
GA-MLxxTPoE+#show policy-map policy1

 Policy Map policy1
  Class Map police
police cir 500 bc 10 pir 1000 be 10 conform-action transmit exceed-action set-dscp-transmit 2 violate-action drop

GA-MLxxTPoE+#
```

This example shows how to display all policy maps at GigabitEthernet 1/0/1.

```
GA-MLxxTPoE+#show policy-map interface gi 1/0/1

 Policy Map: policy1 : output
  Class Map police
police cir 500 bc 10 pir 1000 be 10 conform-action transmit exceed-action set-dscp-
transmit 2 violate-action drop

GA-MLxxTPoE+#
```

5.2.28 wdrr-queue bandwidth

This command is used to set the queue quantum in the WDRR scheduling mode. Use the **no** form of this command to revert to the default setting.

Syntax

- **wdrr-queue bandwidth** *QUANTUM1…QUANTUM8*
- **no wdrr-queue bandwidth**

Parameters

Parameters	Description
QUANTUM1 …QUANTUM8	Specifies the quantum (frame length count) value of every queue for weighted round-robin scheduling.

Default

By default, each quantum value is 1.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

The configuration of this command takes effect when the scheduling mode is in the WDRR mode. Use the **mls qos scheduler wdrr** command to change the scheduling mode to WDRR mode.

Example

This example shows how to configure the queue quantum of the WDRR scheduling mode, queue quantum of queue 0, queue 1, queue 2, queue 3, queue 4, queue 5, queue 6, queue 7 are 1, 2, 3, 4, 5, 6, 7, 8 respectively on GigabitEthernet1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# mls qos scheduler wdrr
GA-MLxxTPoE+(config-if)# wdrr-queue bandwidth 1 2 3 4 5 6 7 8
GA-MLxxTPoE+(config-if)#
```

5.2.29 wrr-queue bandwidth

This command is used to set the queue weight in the WRR scheduling mode. Use the **no** form of this command to revert to the default setting.

Syntax

- **wrr-queue bandwidth** *WEIGHT1…WEIGHT8*
- **no wrr-queue bandwidth**

Parameters

Parameters	Description
WEIGHT1 …WEIGHT8	Specifies the weight (frame count) value of every queue for weighted round-robin scheduling.

Default

By default, the weight value for *WEIGHT1* to *WIGHT7* is 1.
By default, the weight value for *WEIGHT8* is 0.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

The configuration of this command takes effect when the scheduling mode is in the WRR mode. Use the **mls qos scheduler wrr** command to change the scheduling mode to WRR mode. To satisfy the behavior requirements of Expedited Forwarding (EF), the highest queue is always selected by the Per-hop Behavior (PHB) EF and the schedule mode of this queue should be strict priority scheduling. So the weight of the last queue should be zero while the Differentiate Service is supported.

Example

This example shows how to configure the queue weight of the WRR scheduling mode, queue weight of queue 0, queue 1, queue 2, queue 3, queue 4, queue 5, queue 6, queue 7 are 1, 2, 3, 4, 5, 6, 7, 8 respectively on GigabitEthernet1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# mls qos scheduler wrr
GA-MLxxTPoE+(config-if)# wrr-queue bandwidth 1 2 3 4 5 6 7 8
GA-MLxxTPoE+(config-if)#
```

5.3 Storm Control Commands

5.3.1 snmp-server enable traps storm-control

This command is used to enable and configure the sending of SNMP notifications for storm control. Use the no form of this command to disable the sending of SNMP notifications.

Syntax

- snmp-server enable traps storm-control [storm-occur] [storm-clear]
- no snmp-server enable traps storm-control [storm-occur] [storm-clear]

Parameters

Parameters	Description
storm-occur	(Optional) Specifies to send a notification when a storm event is detected.
storm-clear	(Optional) Specifies to send a notification when a storm event is cleared.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

None

Example

This example shows how to enable the sending of traps for storm control for both storm occurrences and clearances.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server enable traps storm-control
GA-MLxxTPoE+(config)#
```

5.3.2 storm-control

This command is used to configure the device to protect the device from broadcast, multicast, and DA unknown packet storm attacks. Use the **no** form of this command to revert to the default settings.

Syntax

- **storm-control** {{**broadcast** | **multicast** | **unicast**} **level** {**pps** *PPS-RISE* [*PPS-LOW*] | **kbps** *KBPS-RISE* [*KBPS-LOW*] | *LEVEL-RISE* [*LEVEL-LOW*]} | **action** {**shutdown** | **drop** | **none**}}
- **no storm-control** {**broadcast** | **multicast** | **unicast** | **action**}

Parameters

Parameters	Description
broadcast	Specifies to set the broadcast rate limit.
multicast	Specifies to set the multicast rate limit.
unicast	Specifies that when the action is configured as the **shutdown** mode, the unicast refers to both known and unknown unicast packet, that is, if the known and unknown unicast packets hit the specified threshold, the port will be shutdown. Otherwise, unicast refers to unknown unicast packets.
level pps *PPS-RISE* [*PPS-LOW*]	Specifies the threshold value in packets count per second. The range is from 1 to 2147483647. If the low PPS value is not specified, the default value is 80% of the specified risen PPS.
level kbps *KBPS-RISE* [*KBPS-LOW*]	Specifies the threshold value as a rate of bits per second at which traffic is received on the port. The range is from 1 to 2147483647. If the low KBPS is not specified, the default value is 80% of the specified risen KBPS.
level *LEVEL-RISE* [*LEVEL-LOW*]	Specifies the threshold value as a percentage of the total bandwidth per port at which traffic is received on the port. The range is from 1 to 100. If the low level is not specified, the default value is 80% of the specified risen level.

Parameters	Description
action shutdown	Specifies to shut down the port when the value specified for rise threshold is reached.
action drop	Specifies to discards packets that exceed the risen threshold.
action none	Specifies not to filter the storm packets.

Default

By default, the broadcast, multicast, and unicast (DLF) storm controls are disabled.
The default action taken when a storm occurs is to drop storm packets.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use the storm control function to protect the network from a storm of broadcast packets, multicast packets, or unknown DA flooding packets. Enter the **storm-control** command to enable storm control for a specific traffic type on the interface.
When the upper threshold is exceeded, logging is performed and the assigned function is performed. If it is below the lower threshold, only logging will be performed.

Example

This example shows how to enable broadcast storm control on GigabitEthernet1/0/1. It sets the threshold of GigabitEthernet1/0/1 to 500 packets per second with the shutdown action.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# storm-control broadcast level pps 500
GA-MLxxTPoE+(config-if)# storm-control action shutdown
GA-MLxxTPoE+(config-if)#
```

5.3.3 storm-control polling

This command is used to configure the polling interval of received packet counts. Use the **no** form of this command to revert to the default settings.

Syntax

- **storm-control polling** {**interval** *SECONDS* | **retries** {*NUMBER* | **infinite**}}
- **no storm-control polling** {**interval** | **retries**}

Parameters

Parameters	Description
interval *SECONDS*	Specifies the polling interval of received packet counts. This value must be between 1 and 300 seconds.
retries *NUMBER*	Specifies the retry count. If the action is configured to the shutdown mode and a storm continues as long as the interval times retries values set, the port will enter the error disabled state. This value must be between 0 and 360. 0 means that a shutdown mode port will directly enter the error disabled state when a storm is detected. **Infinite** means that a shutdown mode port will never enter the error disabled state even if a storm was detected.

Default

The default polling interval is 5 seconds.
The default retries count value is 3.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this to specify the sample interval of received packet counts.

Example

This example shows how to specify the polling interval as 15 seconds.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# storm-control polling interval 15
GA-MLxxTPoE+(config)#
```

5.3.4 show storm-control

This command is used to display the current storm control settings.

Syntax

- **show storm-control interface** *INTERFACE-ID* **[, | -] [broadcast | multicast | unicast]**

Parameters

Parameters	Description
interface *INTERFACE-ID*	Specifies the port's interface ID.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
broadcast	(Optional) Specifies to display the current broadcast storm setting.
multicast	(Optional) Specifies to display the current multicast storm setting.
unicast	(Optional) Specifies to display the current unicast (DLF) storm setting.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

If the interface ID is not specified, all interfaces configurations will be displayed. If the packet type is not specified, all types of storm control settings will be displayed.

Example

This example shows how to display the current broadcast storm control settings.

```
GA-MLxxTPoE+# show storm-control interface gi1/0/1-1/0/6 broadcast

Interface    Action    Threshold         Current    State
-------------------------------------------------------
Gi1/0/1      Drop      500/300 pps       200 pps    Forwarding
Gi1/0/2      Drop      80/64 %           20 %       Forwarding
Gi1/0/3      Drop      80/64 %           70 %       Dropped
Gi1/0/4      Shutdown  60/50 %           20 %       Forwarding
Gi1/0/5      None      60000/50000 kbps  2000 kbps  Forwarding
Gi1/0/6      None      -                 -          Inactive

Total Entries: 6

GA-MLxxTPoE+#
```

This example shows how to display all interface settings for the range from GigabitEthernet 1/0/1 to port 1/0/2.

```
GA-MLxxTPoE+# show storm-control interface Gi 1/0/1-2

Polling Interval       : 15 sec           Shutdown Retries       : Infinite
Trap                   : Disabled
Interface      Storm         Action      Threshold     Current    State
---------------------- ------------------------------------------
Gi1/0/1      Broadcast     Drop         80/64 %       50%        Forwarding
Gi1/0/1      Multicast     Drop         80/64 %       50%        Forwarding
Gi1/0/1      Unicast       Drop         80/64 %       50%        Forwarding
Gi1/0/2      Broadcast     Shutdown     500/300 pps   -          Error Disabled
Gi1/0/2      Multicast     Shutdown     500/300 pps   -          Error Disabled
Gi1/0/2      Unicast       Shutdown     500/300 pps   -          Error Disabled

Total Entries: 6

GA-MLxxTPoE+#
```

Display Parameters

Parameters	Description
Interface	The interface ID.
Action	The configured action, the possible actions are: Drop, Shutdown, None.
Threshold	The configured threshold.

Parameters	Description
Current	The actual traffic rate which is currently flowing though the interface. Its unit may be percentage, kbps, PPS based on the configured meter mode. Because hardware can only counts by PPS, this value of this filed may be a rough value for percentage and kbps.
State	The current state of storm control on a given interface for a given traffic type. The possible states are: **Forwarding:** No storm event has been detected. **Dropped:** A storm event has occurred and the storm traffic exceeding the threshold is dropped. **Error Disabled:** The port is disabled due to a storm. **Link Down:** The port is physically linked down. **Inactive:** Indicates that storm control is not enabled for the given traffic type.

5.4 Filter NetBIOS Commands

5.4.1 deny netbios

This command is used to deny NetBIOS packets on the specified interface. Use the **no** form of this command to revert to the default setting.

Syntax

- **deny netbios**
- **no deny netbios**

Parameters

None.

Default

By default, NetBIOS packets are permitted.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Using this command to deny or permit NetBIOS packets on physical ports.

Example

This example shows how to deny NetBIOS packets on GigabitEthernet1/0/1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#deny netbios
GA-MLxxTPoE+(config-if)#
```

5.4.2 deny extensive-netbios

This command is used to deny NetBIOS packets over 802.3 frame on the specified interface. Use the **no** form of this command to revert to the default setting.

Syntax

- **deny extensive-netbios**
- **no deny extensive-netbios**

Parameters

None.

Default

By default, NetBIOS packets over 802.3 frame are permitted.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for physical ports. Using this command to deny or permit NetBIOS packets over 802.3 frame.

Example

This example shows how to deny NetBIOS packets over 802.3 frame on GigabitEthernet1/0/1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#deny extensive-netbios
GA-MLxxTPoE+(config-if)#
```

5.5 Egress buffer threshold

5.5.1 egress buffer threshold

This command is used to change the egress buffer threshold. Use the **no** form of this command to revert to the default setting.

Syntax

egress buffer threshold {high |mid |low}

no egress buffer threshold

Parameter

Parameters	Description
high	Set the egress buffer threshold to high.
mid	Set the egress buffer threshold to mid.

Default

By default, egress buffer threshold are mid.

Command mode

Global Configuration Mode

Command Default Level

Level：12

Usage Guideline

We recommend that you operate with the default settings regarding the threshold of the output buffering. Change to high only in the environment where traffics, which instantaneously exceed the maximum amount of traffics on the port, occur frequently.

If you change the threshold of the output buffering to high, available functions are limited to VLAN, Link Aggregation (except LACP), Telnet server, IGMP snooping, SNTP client and WEB.

Example

This example shows how a change to high for egress buffer threthold.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#egress buffer threshold high
```

5.5.2 show egress buffer threshold

This command is used to display the current egress buffer threshold.

Syntax

show egress buffer threshold

Parameter

None

Default

None

Command mode

User/Privileged EXEC Mode

Command Default Level

Level：1

Usage Guideline

This command is used to display the current egress buffer threshold.

Example

This example shows how adisplay the current egress buffer threshold.

```
GA-MLxxTPoE+#show egress buffer threshold

Egress Buffer Threshold State: High

GA-MLxxTPoE+#
```

5.6 PTP (Precision Time Protocol)

PTP (Precision Time Protocol) is a function that realizes highly accurate time synchronization in microseconds (one millionth of a second).
Using this function, it is possible to synchronize the time on a packet-based network.

Caution

- Only End to End (E2E) Transparent Clock (TC) mode is supported.
- To use PTP function, Both the PTP setting in global configuration mode and the PTP setting in interface configuration mode should be enabled.
- The PTP function guarantees the time synchronization required for the terminal in cooperation with other devices in the system.
  Time synchronization of the system is not guaranteed only by this model and this function. It is necessary to verify end to end synchronization of the system in advance.

5.6.1 ptp enable（Global）

This command is used to enable the PTP function globally. Use the no form of this command to disable to the function globally.

Syntax

ptp enable

no ptp enable

Parameter

None

Default

By default, this option is disabled.

Command mode

Global Configuration Mode

Command Default Level

Level：12

Usage Guideline

Enables / disables the PTP function.

Example

This example shows how to enable PTP function globally.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#ptp enable
GA-MLxxTPoE+(config)#
```

5.6.2 ptp enable（Interface）

This command is used to enable the PTP function for an interface. Use the **no** form of this command to disable the function for an interface.

Syntax

ptp enable

no ptp enable

Parameter

None

Default

By default, this option is disabled.

Command mode

Interface Configuration Mode

Command Default Level

Level：12

Usage Guideline

This command is used to enable or disable the PTP feature on each physical port.

To use PTP function, Both the PTP setting in global configuration mode and the PTP setting in interface configuration mode should be enabled.
When the PTP function in global configuration mode is disabled or the PTP function in interface configuration mode is disabled, PTP packets are flooded like normal packets.

Example

This example shows how to enable the PTP function on interface Gigabit Ethernet port 1/0/1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#ptp enable
GA-MLxxTPoE+(config-if)#
```

5.6.3 show ptp

This command is used to display the PTP function setting.

Syntax

show ptp

Parameters

None

Default

None

Command Mode

User / Privileged EXEC Mode

Command Default Level

Level : 1

Usage Guideline

This command used to display the PTP settings and status.

Example

This example shows how to display the PTP settings and status.

```
GA-MLxxTPoE+#show ptp

PTP State Setting : Disable
PTP Mode Setting : E2E Transparent Clock

GA-MLxxTPoE+#
```

5.6.4 show ptp interface

This command is used to display the settings of the port on which the PTP function is used.

Syntax

- **show ptp interface** [**interface** *INTERFACE-ID* [, | -]]

Parameters

Parameters	Description
interface *INTERFACE-ID*	(Option)Specify the ID of the interface to be displayed.
,	(Option)Specifies a continuous interface. Alternatively, separate it from the range of the interface.No space is allowed before or after the comma.
-	(Option)Specifies the range of the interface.No space can be used before or after the hyphen.

Default

None

Command Mode

User / Privileged EXEC Mode

Command Default Level

Level : 1

Usage Guideline

This command is used to display the settings of the port on which the PTP function is used.

If no optional parameters are specified, all port information will be displayed. This command displays the PTP function in interface mode even if the PTP function in global configuration mode is disabled.

Example

This example shows how to display the PTP port settings and status.

```
GA-MLxxTPoE+#show ptp interface gi1/0/1-1/0/8

DM?Delay Mechanism
Port    DM      State    Step mode
1/0/1   E2E     Disable  one step
1/0/2   E2E     Disable  one step
1/0/3   E2E     Disable  one step
1/0/4   E2E     Disable  one step
1/0/5   E2E     Disable  one step
1/0/6   E2E     Disable  one step
1/0/7   E2E     Disable  one step
1/0/8  E2E      Disable  one step
```

6 Network Monitoring

6.1 SPAN

6.1.1 monitor session destination interface

This command is used to configure the destination interface for a monitor session, allowing packets on source ports to be monitored via a destination port. Use the **no** form of this command to remove the destination interface of the session.

Syntax

- **monitor session** *SESSION-NUMBER* **destination interface** *INTERFACE-ID*
- **no monitor session** *SESSION-NUMBER* **destination interface** *INTERFACE-ID*

Parameters

Parameters	description
SESSION-NUMBER	Specifies the session number for the monitor session. The valid range is 1 to 4.
INTERFACE-ID	Specifies the destination interface for the monitor session.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use this command to configure the destination interface for a local monitor session or the destination interface on the destination switch for an RSPAN session.

Both physical ports and port channels are valid as destination interfaces for monitor sessions. For a monitor session, multiple source interfaces can be specified, but only one destination interface can be specified. An interface cannot be a source interface of one session and destination port of another session simultaneously. An interface can be configured as the destination interface of multiple sessions, but it can be a source interface of only one session.
To configure the destination switch of an RSPAN session, also use the **monitor session source remote vlan** command to configure the VLAN that the monitored source packets are tunneled to from the remote site.

Example

This example shows how to create a port monitor session with the session number 1. It assigns a physical port GigabitEternet1/0/1 as the destination port and three physical source ports (GigabitEthernet1/0/2 to GigabitEthernet1/0/4) as monitor source ports.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# monitor session 1 destination interface gi1/0/1
GA-MLxxTPoE+(config)# monitor session 1 source interface gi1/0/2-4
GA-MLxxTPoE+(config)#
```

6.1.2 monitor session destination remote vlan

This command is used to configure the RSPAN VLAN and destination port for an RSPAN source session. Use the **no** form of this command to remove the configuration of the RSPAN VLAN.

Syntax

- **monitor session** *SESSION-NUMBER* **destination remote vlan** *VLAN-ID* **interface** *INTERFACE-ID*
- **no monitor session** *SESSION-NUMBER* **destination remote vlan [access-list** *ACCESS-LIST-NAME*]

Parameters

Parameters	description
SESSION-NUMBER	Specifies the session number for the monitor session. The valid range is 1 to 4.
VLAN-ID	Specifies the RSPAN VLAN used to tunnel the monitored packets to the remote site. The valid range is 2 to 4094.
interface *INTERFACE-ID*	Specifies the interface to transmit the monitored packets to the remote site.

Parameters	description
access-list *ACCESS-LIST-NAME*	(Optional) Specifies the flow used to perform egress per flow RSPAN VLAN replacement. The flow will still be configured even if the access list does not exist.
replace vlan *VLAN-ID*	(Optional) Specifies the VLAN ID used to replace the RSPAN VLAN ID for the matched flow of packets transmitted out from the destination port on a RSPAN source switch. The valid range is from 1 to 4094.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use this command on the source switch of an RSPAN session.
The **monitor session destination remote vlan** command configures the destination port used to transmit the monitor packets and the RSPAN VLAN used to tag the monitored packets to the remote site. For each session, only one destination interface can be configured. The destination port does not need to be a member port of the RSPAN VLAN. The destination port can be either a physical port or a port channel.
Each session should be configured with a unique RSPAN VLAN. An interface cannot be specified for the command to transmit the monitored packets for multiple RSPAN sessions.
A flow can be defined by specifying an access list to be matched against the packets monitored by the session. The RSPAN VLAN ID is used to tunnel these packets and will be replaced by the Replace VLAN ID. For an RSPAN source session, multiple VLAN replacement flows can be configured. For remote sessions, it is suggested that the RSPAN VLAN is configured for dedicated use to monitor traffic only.
Use the **monitor session source interface** command to configure the source ports whose packets will be monitored.
Use the **remote-span** command in the VLAN configuration mode to specify a VLAN as an RSPAN VLAN. The monitored packet will be tunneled over the trunk member port of the RSPAN VLAN in the subsequent switches.

Example

This example shows how to create an RSPAN session on the source switch. It assigns VLAN 100 as the RSPAN VLAN with the destination GigabitEthernet1/0/6 and three source ports (GigabitEthernet1/0/2, GigabitEthernet1/0/3 and GigabitEthernet1/0/4) as the port being monitored.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# monitor session 2 source interface gi1/0/2-4
GA-MLxxTPoE+(config)# monitor session 2 destination remote vlan 100 interface gi1/0/6
GA-MLxxTPoE+(config)#
```

6.1.3 monitor session source interface

This command is used to configure the source port of a monitor session. Use the **no** form of this command to remove a source port from the monitor session.

Syntax

- **monitor session** *SESSION-NUMBER* **source interface** {*INTERFACE-ID* [**,** | **-**] [**both** | **rx** | **tx**] | **cpu rx**}
- **no monitor session** *SESSION-NUMBER* **source interface** {*INTERFACE-ID* [**,** | **-**] | **cpu rx**}

Parameters

Parameters	description
SESSION-NUMBER	Specifies the session number for the monitor session. The valid range is 1 to 4.
interface *INTERFACE-ID*	Specifies the source interface for a monitor session.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
both	(Optional) Specifies to monitor the packets transmitted and received on the port.
rx	(Optional) Specifies to monitor the packets received on the port.
tx	(Optional) Specifies to monitor the packets transmitted on the port.
cpu rx	Specifies the CPU receiving mirror. All packets received by the CPU are mirrored.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Both physical ports and port channels are valid as source interfaces of monitor sessions.
For a monitor session, multiple source interfaces can be specified, but only one destination interface can be specified. An interface cannot be a source interface of one session and destination port of another session simultaneously. An interface can be configured as destination interface of multiple sessions, but it can be a source interface of only one session.
If the direction is not specified, both transmitted and received traffic are monitored. This is the same as specifying **both**.

NOTE For mirror packets in the Tx direction, the VLAN tag of the received VLAN ID is added.

Example

This example shows how to create a port monitor session with session number 1. It assigns a physical port gi1/0/1 as a destination port and three source physical ports (gi1/0/2 to gi1/0/4) as monitor source ports.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# monitor session 1 destination interface gi1/0/1
GA-MLxxTPoE+(config)# monitor session 1 source interface gi1/0/2-4
GA-MLxxTPoE+(config)#
```

6.1.4 monitor session source acl

This command is used to configure an access list for flow-based monitoring. Use the **no** form of this command to remove an access list for flow-based monitoring.

Syntax

- **monitor session** *SESSION-NUMBER* **source acl** *ACCESS-LIST-NAME*

- **no monitor session** *SESSION-NUMBER* **source acl** *ACCESS-LIST-NAME*

Parameters

Parameters	description
SESSION-NUMBER	Specifies the session number for the monitor session. The valid range is 1 to 4.
ACCESS-LIST-NAME	Specifies the flow-based mirror. Only the ingress mirror is supported and only MAC, IP, or IPv6 access lists can be monitored. Even if the access list does not exist, the flow-based mirror can still be configured.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Only one access list can be monitored on a session at a time (One access list can include multiple flows). When an access list is monitored, the packet filtered by the access list that is applied to the hardware via the **access-group** or **vlan map** command will be monitored.

Example

This example shows how to create a monitor session with the session number 2. It assigns the MAC access list "MAC-Monitored-flow" as the monitor source.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# monitor session 2 destination interface gi1/0/1
GA-MLxxTPoE+(config)# monitor session 2 source acl MAC-Monitored-flow
GA-MLxxTPoE+(config)#
```

6.1.5 monitor session source remote vlan

This command is used to configure the RSPAN VLAN for an RSPAN destination session. Use the **no** form of this command to remove the configuration.

Syntax

- monitor session *SESSION-NUMBER* source remote vlan *VLAN-ID*
- no monitor session *SESSION-NUMBER* source remote vlan

Parameters

Parameters	description
SESSION-NUMBER	Specifies the session number of the monitor session. The valid range is 1 to 4.
VLAN-ID	Specifies the VLAN that the monitored source packets are tunneled over from the remote site. The valid range is 2 to 4094.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

Use this command on the destination switch of an RSPAN session.
The **monitor session source remote vlan** command configures the VLAN that the monitored source packets are tunneled to from the remote site. Use the **monitor session destination interface** command to configure the destination port to transmit the monitored packets to.
Each session should be configured with a unique RSPAN VLAN. Use the **remote-span** command in the VLAN configuration mode to specify a VLAN as an RSPAN VLAN.

Example

This example shows how to create an RSPAN session on the destination switch. It assigns VLAN 100 as the RSPAN VLAN and GigabitEthernet1/0/4 as the destination port. It also assigns VLAN 100 as the RSPAN VLAN. The monitored packets arrive at GigabitEthernet2/0/1 and will be transmitted out from port GigabitEthernet2/0/4.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 100
GA-MLxxTPoE+(config-vlan)# remote-span
GA-MLxxTPoE+(config-vlan)#exit
GA-MLxxTPoE+(config)# interface gi2/0/1
GA-MLxxTPoE+(config-if)# switchport mode trunk
GA-MLxxTPoE+(config-if)# switchport trunk allowed vlan 100
GA-MLxxTPoE+(config-if)# exit
GA-MLxxTPoE+(config)# interface gi1/0/4
GA-MLxxTPoE+(config-if)# switchport mode access
GA-MLxxTPoE+(config-if)# switchport access vlan 100
GA-MLxxTPoE+(config-if)# exit
GA-MLxxTPoE+(config)# monitor session 2 source remote vlan 100
GA-MLxxTPoE+(config)# monitor session 2 destination interface gi2/0/4
GA-MLxxTPoE+(config)#
```

6.1.6 remote-span

This command is used to specify a VLAN as an RSPAN VLAN. Use the **no** form of this command to revert to a non-RSPAN VLAN.

Syntax

- **remote-span**
- **no remote-span**

Parameters

None

Default

By default, 802.1Q VLAN is used.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12

Usage Guidelines

Use the **remote-span** command in the VLAN configuration mode to specify a VLAN as an RSPAN VLAN. When a VLAN is specified as an RSPAN VLAN, the MAC address learning option on the RSPAN VLAN is disabled. Use this command on any of the intermediate switches and the destination switch involved in the RSPAN session.
For any of the intermediate switches involved in a RSPAN session, the port that the monitored packets arrive on and the port that the monitored packets leave from need to be configured as tagged member ports of the RSPAN VLAN.

Example

This example shows how to assign VLAN 100 as the RSPAN VLAN on an intermediate switch in the RSPAN session. Interface GigabitEthernet1/0/1 is where the monitored packets arrive on and GigabitEthernet1/0/5 is where the monitored packets leave from.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface ethernet1/0/1
GA-MLxxTPoE+(config-if)# switchport mode trunk
GA-MLxxTPoE+(config-if)# switchport trunk allowed vlan 100
GA-MLxxTPoE+(config-if)# exit
GA-MLxxTPoE+(config)# interface ethernet1/0/5
GA-MLxxTPoE+(config-if)# switchport mode trunk
GA-MLxxTPoE+(config-if)# switchport trunk allowed vlan 100
GA-MLxxTPoE+(config-if)# exit
GA-MLxxTPoE+(config)# vlan 100
GA-MLxxTPoE+(config-vlan)# remote-span
GA-MLxxTPoE+(config-vlan)#
```

6.1.7 no monitor session

This command is used to delete a monitor session.

Syntax

- **no monitor session** *SESSION-NUMBER*

Parameters

Parameters	description
SESSION-NUMBER	Specifies the session number of the monitor session to be deleted. The valid range is from 1 to 4.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

If a monitor session is deleted, all configuration for the session is removed.

Example

This example shows how to delete the monitor session with session number 1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# no monitor session 1
GA-MLxxTPoE+(config)#
```

6.1.8 show monitor session

This command is used to display all or a specific monitor session.

Syntax

- **show monitor session** [*SESSION-NUMBER* | **remote** | **local**]

Parameters

Parameters	description
SESSION-NUMBER	(Optional) Specifies the session number which you want to display.
local	(Optional) Specifies to display the local session.
remote	(Optional) Specifies to display the remote RSPAN session.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1.

Usage Guidelines

If this command is used without specifying a session number, all monitor sessions are displayed.

Example

This example shows how to display a port monitor session with the session number 1.

```
GA-MLxxTPoE+#show monitor session

 Session 1
     Session Type: local session
     Destination Port: Ethernet1/0/1
     Source Ports:
         Both:
             Ethernet1/0/2
             Ethernet1/0/3
             Ethernet1/0/4

 Total Entries: 1

GA-MLxxTPoE+#
```

6.2 Remote Network Monitoring (RMON) Commands

6.2.1 rmon collection stats

This command is used to enable RMON statistics on the configured interface. Use the **no** form of this command to disable the RMON statistics.

Syntax

- **rmon collection stats** *INDEX* [**owner** *NAME*]
- **no rmon collection stats** *INDEX*

Parameters

Parameters	Description
INDEX	Specifies the RMON table index. The range is from 1 to 65535.
owner *NAME*	Specifies the owner string. The maximum length is 127.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

This command is only available for physical port interface configuration. The RMON statistics group entry number is dynamic. Only the interface that is enabled for RMON statistics will have a corresponding entry in the table.

Example

This example shows how to configure an RMON statistics entry with an index of 65 and the owner name “guest” on GigabitEthernet1/0/2.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/2
GA-MLxxTPoE+(config-if)# rmon collection stats 65 owner guest
GA-MLxxTPoE+(config-if)#
```

6.2.2 rmon collection history

This command is used to enable RMON MIB history statistics gathering on the configured interface. Use the **no** form of this command to disable history statistics gathering on the interface.

Syntax

- **rmon collection history** *INDEX* [**owner** *NAME*] [**buckets** *NUM*] [**interval** *SECONDS*]
- **no rmon collection history** *INDEX*

Parameters

Parameters	Description
INDEX	Specifies the history group table index. The range is from 1 to 65535.
owner *NAME*	Specifies the owner string. The maximum length is 127.
buckets *NUM*	Specifies the number of buckets specified for the RMON collection history group of statistics. If not specified, the default is 50. The range is from 1 to 65535.
interval *SECONDS*	Specifies the number of seconds in each polling cycle. The range is from 1 to 3600.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

This command is only available for physical port interface configuration. The RMON history group entry number is dynamic. Only the interface that is enabled for RMON history statistics gathering will have a corresponding entry in the table. The configured interface becomes the data source for the created entry.

Example

This example shows how to enable the RMON MIB history statistics group on GigabitEthernet1/0/8.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/8
GA-MLxxTPoE+(config-if)# rmon collection history 101 owner it@domain.com interval
2000
GA-MLxxTPoE+(config-if)#
```

6.2.3 rmon alarm

This command is used to configure an alarm entry to monitor an interface. Use the **no** form of this command to remove an alarm entry.

Syntax

- **rmon alarm** *INDEX VARIABLE INTERVAL* {**delta** | **absolute**} **rising-threshold** *VALUE* [*RISING-EVENT-NUMBER*] **falling-threshold** *VALUE* [*FALLING-EVENT-NUMBER*] [**owner** *STRING*]
- **no rmon alarm** *INDEX*

Parameters

Parameters	Description
INDEX	Specifies the alarm index. The range is from 1 to 65535.
VARIABLE	Specifies the object identifier of the variable to be sampled.
INTERVAL	Specifies the interval in seconds for the sampling of the variable and checking against the threshold. The valid range is from 1 to 2147483647.
delta	Specifies that the delta of two consecutive sampled values is monitored.
absolute	Specifies that the absolute sampled value is monitored.
rising-threshold *VALUE*	Specifies the rising threshold. The valid range is from 0 to 4294967295.

Parameters	Description
RISING-EVENT-NUMBER	(Optional) Specifies the index of the event entry that is used to notify the ringing threshold crossing event. The valid range is from 1 to 65535. If not specified, no action is taken while crossing the ringing threshold.
falling-threshold *VALUE*	Specifies the falling threshold. The valid range is from 0 to 2147483647.
FALLING-EVENT-NUMBER	(Optional) Specifies the index of the event entry that is used to notify the falling threshold crossing event. The valid range is from 1 to 65535. If not specified, no action is taken while crossing the falling threshold.
owner *STRING*	(Optional) Specifies the owner string. The maximum length is 127.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

The RMON alarm facility periodically takes samples of the value of variables and compares them against the configured threshold.

Example

This example shows how to configure an alarm entry to monitor an interface.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# rmon alarm 783 1.3.6.1.2.1.2.2.1.12.6 30 delta rising-threshold
20 1 falling-threshold 10 1 owner Name
GA-MLxxTPoE+(config)#
```

6.2.4 rmon event

This command is used to configure an event entry. Use the **no** form of this command to remove an event entry.

Syntax

- rmon event *INDEX* [log] [[trap *COMMUNITY*] [owner *NAME*] [description *TEXT*]
- no rmon event *INDEX*

Parameters

Parameters	Description
INDEX	Specifies the index of the alarm entry. The valid range is from 1 to 65535.
log	(Optional) Specifies to generate log message for the notification.
trap *COMMUNITY*	(Optional) Specifies to generate SNMP trap messages for the notification. The maximum length is 30.
owner *NAME*	(Optional) Specifies the owner string. The maximum length is 30.
description *STRING*	(Optional) Specifies a description for the RMON event entry. Enter a text string with a maximum length of 127 characters.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guidelines

If the log parameter is specified, but not the trap parameter, the created entry will cause a log entry to be generated on an event occurrence. If the trap parameter is specified, but not the log parameter, the created entry will cause an SNMP notification to be generated on an event occurrence.
If both log and trap are specified, the created entry will cause both the log entry and the SNMP notification to be generated on event occurrence.

Example

This example shows how to configure an event with an index of 13 to generate a log on the occurrence of the event.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# rmon event 13 log owner it@domain.com description
ifInNUcastPkts is too much
GA-MLxxTPoE+(config)#
```

6.2.5 show rmon alarm

This command is used to display the alarm configuration.

Syntax

- show rmon alarm

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guidelines

This command displays the RMON alarm table.

Example

This example shows how to display the RMON alarm table.

```
GA-MLxxTPoE+# show rmon alarm

Alarm index 23, owned by IT
  Monitors OID: 1.3.6.1.2.1.2.2.1.10.1
  every 120 second(s)
  Taking delta samples, last value was 2500
  Rising threshold is 2000, assigned to event 12
  Falling threshold is 1100, assigned to event 12
  On startup enable rising or falling alarm

GA-MLxxTPoE+#
```

6.2.6 show rmon events

This command is used to display the RMON event table.

Syntax

- show rmon events

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guidelines

This command displays the RMON event table.

Example

This example shows how to display the RMON event table.

```
GA-MLxxTPoE+# show rmon events

Event 1, owned by manager1
  Description is Errors
  Event trigger action: log & trap sent to community manager
  Last triggered time: 13:12:15, 2017-03-02

Event 2, owned by manager2
  Description is Errors
  Event trigger action: log & trap
  Last triggered time:

GA-MLxxTPoE+#
```

6.2.7 show rmon history

This command is used to display RMON history statistics information.

Syntax

- show rmon history

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guidelines

This command displays the history of the statistics for all of the configured entries.

Example

This example shows how to display RMON Ethernet history statistics.

```
GA-MLxxTPoE+#show rmon history

Index 23 owned by Manager Data source is Gi1/0/2
  Interval: 30 seconds
  Requested buckets: 50, Granted buckets: 50
GA-MLxxTPoE+#
```

6.2.8 show rmon statistics

This command is used to display RMON Ethernet statistics.

Syntax

- show rmon statistics

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guidelines

Statistics for all of the configured entries are displayed.

Example

This example shows how to display the RMON statistics.

```
GA-MLxxTPoE+# show rmon statistics

Index 32, owned by it@domain.com, Data Source is  gigabitgi1/0/2
    Received Octets : 234000, Received packets : 9706
    Broadcast packets: 2266, Multicast packets: 192
    Undersized packets: 213, Oversized  packets: 24
    Fragments: 2, Jabbers: 1
    CRC alignment errors: 0, Collisions: 0
    Drop events : 0
    Packets in 64 octets: 256, Packets in 65-127 octets : 236
    Packets in 128-255 octets : 129, Packets in 256-511 octets : 10
    Packets in 512-1023 octets : 38, Packets in 1024-1518 octets : 2200

GA-MLxxTPoE+#
```

6.3 sFlow

6.3.1 sflow collector

Use this command to create the definition of the sFlow collector. To delete the collector definition, use no form of this command.

Syntax

- **sflow collector IP** *IP-ADDRESS* [**port** *port*]
- **no sflow collector IP** *IP-ADDRESS*

Parameter

Parameter	Description
IP *IP-ADDRESS*	This parameter specifies the host IPv4 address, which is used as a sFlow collector.
port *port*	This parameter specifies the port number of (optional) sFlow messages. If you do not specify it, the port-number is set to 6,343 as the default settings. The range is from 1 to 65,535.

Default Settings

A receiver is not defined.

Command Mode

Global Configuration Mode

Usage Guidelines

Use this command to create the definition of the sFlow collector.

Example

The following example shows the method of configuring 192.168.22.44 as a host IP address of the sFlow collector.

```
GA-MLxxTPoE+(config)# sflow collector IP 192.168.22.44
```

6.3.2 sflow sampler rate

Use this command to enable the sFlow flow-sampling of the specific port, and then configure the sFlow sampling rate to check how many frames are needed per sampling. To disable the flow sampling, use **no** form of the command.

Syntax

- **sflow sampler rate** *rate* **interface** *INTERFACE-ID [, | -]*
- **no sampler rate**

Parameter

Parameter	Description
rate	This parameter specifies the sFlow sampling rate to check how many frames are needed per sampling. The sFlow sampling rate is calculated by 1/rate; the range is from 1,024 to 65,536.
interface *INTERFACE-ID*	This parameter specifies the interface, which enables the sFlow flow-sampling. The valid interface is a physical interface.
,	This parameter specifies the (optional) consecutive interfaces, or separates the range of an interface from the previous range. You cannot use any spaces before and after a comma.
-	This parameter specifies the range of an (optional) interface. You cannot use any spaces before and after a hyphen.

Default Settings

None

Command Mode

Global Configuration Mode

Usage Guidelines

Use this command to enable the sFlow flow-sampling of the specific port, and then configure the sFlow sampling rate.

Example

In the example below, enable the sFlow flow sampling of GigabitEthernet1/0/1 and 1/0/2, and then set the sFlow sampling rate to 1/1024.

```
GA-MLxxTPoE+# sflow sampler rate 1024 interface gi1/0/1-1/0/2
```

6.3.3 sflow sampler poller-interval

Use this command to enable the sFlow counter sampling of the specific port, and then configure the polling-interval of the sFlow counter. To disable the sFlow counter sampling, use no form of the command.

Syntax

- **sflow sampler poller-interval** *interval* **interface** *INTERFACE-ID [, | -]*
- **no sflow sampler poller-interval**

Parameter

Parameter	Description
interval	This parameter specifies the polling-interval (seconds) of the sFlow counter; the range is from 0 to 86,400. If the polling-interval is set to 0, the sFlow counter sample is not transmitted.
interface *INTERFACE-ID*	This parameter specifies the interface, which enables the sFlow counter sampling. The valid interface is a physical interface.
,	This parameter specifies the (optional) consecutive interfaces, or separates the range of an interface from the previous range. You cannot use any spaces before and after a comma.
-	This parameter specifies the range of an (optional) interface. You cannot use any spaces before and after a hyphen.

Default Settings

Disabled

Command Mode

Global Configuration Mode

Usage Guidelines

Use this command to enable the sFlow counter sampling of the specific port, and then configure the polling-interval of the sFlow counter.

Example

In the example below, enable the sFlow counter sampling of GigabitEthernet 1/0/1 and 1/0/2, and then set the polling-interval of the sFlow counter to 60 seconds.

```
GA-MLxxTPoE+(config)# sflow sampler poller-interval 60 interface gi1/0/1-1/0/2
```

6.3.4 show sflow information

Use this command to display the sFlow settings.

Syntax

- show sflow information

Parameter

None

Command Mode

Privileged Mode

Usage Guidelines

Use this command to display the sFlow settings.

Example

The following example shows the method of displaying the sFlow settings.

```
GA-MLxxTPoE+# show sflow information

 Collector IP                  : 192.16.22.44
 Collector UDP Port            : 6343
 Sampler Rate                  : 1024
 Sampler Data Source Interface : Gi1/0/1-1/0/2
 Sampler Poller interval       : 60 Sec.
 Sampler Poller Interface      : Gi1/0/1-1/0/2

GA-MLxxTPoE+#
```

7 IP Setting

7.1 Basic IPv4 Commands

7.1.1 ip address

This command is used to set a primary or secondary IPv4 address for an interface, or acquire an IP address on an interface from the DHCP. Use the **no** form of this command to remove the configuration of an IP address or disable DHCP on the interface.

Syntax

- **ip address** {*IP-ADDRESS SUBNET-MASK* | **dhcp**}
- **no ip address** [*IP-ADDRESS SUBNET-MASK* | **dhcp**]

Parameters

Parameters	Description
IP-ADDRESS	Specifies the IP address.
SUBNET-MASK	Specifies the subnet mask for the associated IP address.
dhcp	Specifies to acquire an IP address configuration on an interface from the DHCP protocol.

Default

The default IP address for VLAN 1 is 0.0.0.0/0.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The IPv4 address of an interface can be either manually assigned by the user or dynamically assigned by the DHCP server. Use the **no ip address** command to delete the configured IP address entry.

Example

This example shows how to set 10.108.1.27 for VLAN1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface vlan1
GA-MLxxTPoE+(config-if)#ip address 10.108.1.27 255.255.255.0
GA-MLxxTPoE+(config-if)#
```

7.1.2 ip route

This command is used to create a static route entry. Use the **no** form of this command to remove a static route entry.

Syntax

- **ip route** *NETWORK-PREFIX NETWORK-MASK IP-ADDRESS*
- **no ip route** *NETWORK-PREFIX NETWORK-MASK IP-ADDRESS*

Parameters

Parameters	Description
NETWORK-PREFIX	Specifies the network address.
NETWORK-MASK	Specifies the network mask.
IP-ADDRESS	Specifies the IP address of the next hop that can be used to reach destination network.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use **0.0.0.0 0.0.0.0** to specify the default route.

Example

This example shows how to add default gateway as 10.1.1.254.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.254
GA-MLxxTPoE+(config)#
```

7.1.3 arp

This command is used to add a static entry in the Address Resolution Protocol (ARP) cache. Use the **no** form of this command to remove a static entry in the ARP cache.

Syntax

- **arp** *IP-ADDRESS HARDWARE-ADDRESS*
- **no arp** *IP-ADDRESS HARDWARE-ADDRESS*

Parameters

Parameters	Description
IP-ADDRESS	Specifies the network layer IP address.
HARDWARE-ADDRESS	Specifies the local data-link Media Access (MAC) address (a 48-bit address).

Default

No static entries are installed in the ARP cache.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The ARP table keeps the network layer IP address to local data-link MAC address association. The association is kept so that the addresses will not have to be repeatedly resolved. Use this command to add static ARP entries.

Example

This example shows how to add a static ARP entry for a typical Ethernet host.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# arp 10.31.7.19 0050.4000.1834
GA-MLxxTPoE+(config)#
```

7.1.4 arp timeout

This command is used to set the ARP aging time for the ARP table. Use the **no** form of this command to revert to the default setting.

Syntax

- **arp timeout** *MINUTES*
- **no arp timeout**

Parameters

Parameters	Description
MINUTES	Specifies the dynamic entry that will be aged-out if it has no traffic activity within the timeout period. The valid values are from 0 to 65535. If this value is configured as 0, then ARP entries will never age out.

Default

The default value is 240 minutes.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Used to set the ARP aging time for the ARP table. Use the **no** command to revert to default setting.

Example

This example shows how to set the ARP timeout to 60 minutes to allow entries to time out more quickly than the default setting.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface vlan1
GA-MLxxTPoE+(config-if)# arp timeout 60
GA-MLxxTPoE+(config-if)#
```

7.1.5 clear arp-cache

This command is used to clear the dynamic ARP entries from the table.

Syntax

- **clear arp-cache** {**all** | *IP-ADDRESS*}

Parameters

Parameters	Description
all	Specifies to clear the dynamic ARP cache entries associated with all interfaces.
IP-ADDRESS	Specifies the IP address of the specified dynamic ARP cache entry that will be cleared.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to delete dynamic entries from the ARP table. The user can select to delete all dynamic entries, specific dynamic entries, or all of the dynamic entries that are associated with a specific interface.

Example

This example shows how to remove all dynamic entries from the ARP cache.

```
GA-MLxxTPoE+# clear arp-cache all
GA-MLxxTPoE+#
```

7.1.6 show ip interface

This command is used to display the IP interface information.

Syntax

- **show ip interface** [*INTERFACE-ID*] **[brief]**

Parameters

Parameters	Description
INTERFACE-ID	(Optional) Specifies to display information for the specified IP interface.
brief	(Optional) Specifies to display a summary of the IP interface information.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

If no parameter is specified, information for all the interfaces will be displayed.

Example

This example shows how to display the brief information of the IP interface.

```
GA-MLxxTPoE+#show ip interface brief

Interface    IP Address      Link Status
---------- ---------------  -----------
vlan1       10.90.90.90      up

Total Entries: 1

GA-MLxxTPoE+#
```

This example shows how to display the IP interface information for VLAN 1.

```
GA-MLxxTPoE+#show ip interface vlan 1

Interface vlan1 is enabled, Link status is up
  IP address is 10.90.90.90/24 (Manual)
  ARP timeout is 240 minutes.
  gratuitous-send is disabled, interval is 0 seconds

Total Entries: 1

GA-MLxxTPoE+#
```

7.1.7 show ip route

This command is used to display the entry in the routing table.

Syntax

- **show ip route [***PROTOCOL***]**

Parameters

Parameters	Description
PROTOCOL	(Optional) Specifies the following keywords: static, connected.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command is used to display the entry in the routing table.

Example

This example shows how to display the routing table.

```
GA-MLxxTPoE+#show ip route
Code: C - connected, S - static
      * - candidate default

Gateway of last resort is 10.1.1.254 to network 0.0.0.0

C    10.0.0.0/8 is directly connected, vlan1

Total Entries: 1

GA-MLxxTPoE+#
```

7.1.8 show ip route summary

This command is used to display the brief information for the working routing entries.

Syntax

- show ip route summary

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command displays the brief information for the working routing entries.

Example

This example shows how to display the brief information for the working routing entries.

```
GA-MLxxTPoE+#show ip route summary

Route Source    Networks
Connected       3
Static          1
Total           14

GA-MLxxTPoE+#
```

7.1.9 show arp

This command is used to display the ARP cache.

Syntax

- **show arp** [*ARP-TYPE*] [**ip-address** [*MASK*]] [*INTERFACE-ID*] [*HARDWARE-ADDRESS*]

Parameters

Parameters	Description
ARP-TYPE	(Optional) Specifies the ARP type. **dynamic** – Specifies to display only dynamic ARP entries. **static** –Specifies to display only static ARP entries.
IP-ADDRESS [*MASK*]	(Optional) Specifies to display a specific entry or entries that belong to a specific network.
INTERFACE-ID	(Optional) Specifies to display ARP entries that are associated with a specific network.
HARDWARE-ADDRESS	(Optional) Specifies to display ARP entries whose hardware address equal to this address

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Used to display a specific ARP entry, all ARP entries, dynamic entries, or static entries, or entries associated with an IP interface.

Example

This example shows how to display the ARP cache.

```
GA-MLxxTPoE+# show arp

S - Static Entry
IP Address                  Hardware Addr       IP Interface     Age (min)
------------------------------------------------------------------------------
S 10.108.42.112             00-50-40-10-4b-af   vlan100          forever
10.108.42.114               00-50-40-10-85-9b   vlan200          forever
10.108.42.121               00-50-40-10-68-cd   vlan300          125

Total Entries: 3

GA-MLxxTPoE+#
```

7.1.10 show arp timeout

This command is used to display the aging time of ARP cache.

Syntax

- **show arp timeout [interface** *INTERFACE-ID*]

Parameters

Parameters	Description
interface *INTERFACE-ID*	(Optional) Specifies the interface ID.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command is used to display the configured ARP aging time.

Example

This example shows how to display the ARP aging time.

```
GA-MLxxTPoE+#show arp timeout


Interface    Timeout (minutes)
------------ -----------------
vlan1        60
------------ -----------------

Total Entries: 1


GA-MLxxTPoE+#
```

7.2 Basic IPv6 Commands

7.2.1 clear ipv6 neighbors

This command is used to clear IPv6 neighbor cache dynamic entries.

Syntax

- **clear ipv6 neighbors {all | interface** *INTERFACE-ID* **}**

Parameters

Parameters	Description
all	Specifies to clear the dynamic neighbor cache entries associated with all interfaces.
INTERFACE-ID	Specifies to clear dynamic neighbor cache entries associated with the specified interface will be cleared.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level：12

Usage Guideline

This command will only clear dynamic neighbor cache entries.

Example

This example shows hoe to clear IPv6 neighbor cache entries associated with interface VLAN 1.

```
GA-MLxxTPoE+# clear ipv6 neighbors interface vlan1
GA-MLxxTPoE+#
```

7.2.2 ipv6 address

This command is used to manually configure an IPv6 addresses on the interface. Use the **no** form of this command to delete a manually configured IPv6 address.

Syntax

- **ipv6 address {***IPV6-ADDRESS/PREFIX-LENGTH* **|** *PREFIX-NAME SUB-BITS/PREFIX-LENGTH* **|** *IPV6-ADDRESS* **link-local}**
- **no ipv6 address {***IPV6-ADDRESS/PREFIX-LENGTH* **|** *PREFIX-NAME SUB-BITS/PREFIX-LENGTH* **|** *IPV6-ADDRESS* **link-local}**

Parameters

Parameters	Description
IPV6-ADDRESS	Specifies the IPv6 address and the length of prefix for the subnet.
PREFIX-LENGTH	Specifies the length of the prefix. The prefix of the IPv6 address is also a local subnet on the interface.
PREFIX-NAME	Specifies the name of the prefix with a maximum of 12 characters.The syntax allows characters for general string, but does not allow spaces.
SUB-BITS	Specifies the sub-prefix part and host part of the IPv6 address.
link-local	Specifies a link-local address to be configured.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level：12

Usage Guideline

The IPv6 address can directly be specified by the user or configured based on a general prefix. The general prefix can be acquired by the DHCPv6 client. The

general prefix does not need to exist before it can be used in the ipv6 address command. The IPv6 address will not be configured until the general prefix is acquired. The configured IPv6 address will be removed when the general prefix is timeout or removed. The general prefix IPv6 address is formed by the general prefix in the leading part of bits and the sub-bits excluding the general prefix part in the remaining part of bits.
An interface can have multiple IPv6 addresses assigned using a variety of mechanisms, including manual configuration, stateless address configuration, and stateful address configuration.
When the IPv6 address is configured on an interface, IPv6 processing is enabled for the interface. The prefix of the configured IPv6 address will automatically be advertised as prefix in the RA messages transmitted on the interface.

Example

This example shows how to configure an IPv6 address.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface vlan2
GA-MLxxTPoE+(config-if)# ipv6 address 3ffe:22:33:44::55/64
```

This example shows hoe to remove an IPv6 address.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface vlan2
GA-MLxxTPoE+(config-if)# no ipv6 address 3ffe:22:3:44::55/64
```

7.2.3 ipv6 route

This command is used to create an IPv6 static route entry. Use the **no** command to remove an IPv6 static route entry.

Syntax

- **ipv6 route default {[***NETWORK-PREFIX/PREFIX-LENGTH***]} | [***INTERFACE-ID***] }**
- **no ipv6 route default{[***NETWORK-PREFIX/PREFIX-LENGTH***]} | [***INTERFACE-ID***] }**

Parameters

Parameters	Description
NETWORK-PREFIX/PREFIX-LENGTH	This parameter specifies the prefix-length of the network prefix and static route.
INTERFACE-ID	(Optional) This parameter specifies the forwarding interface, which corresponds with the packet routing.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Floating state route is supported. This means that there could have two routes with the same destination network address but different next hop. If none of the **primary** or **backup** parameter is specified, the static route will be automatically determined to be a primary route or a backup route. Primary route is preferable, and is always used for forwarding when it is active. When the primary route is down, the backup route will be used.

Example

This example shows how to create a static route destined for the network where proxy server resides.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#ipv6 route default vlan1 fe80::0000:00ff:1111:2233
GA-MLxxTPoE+(config)#
```

7.2.4 ipv6 address eui-64

This command is used to configure an IPv6 address on the interface using the EUI-64 interface ID. Use the **no** form of this command to delete an IPv6 address formaed by the EUI-64 interface ID.

Syntax

- **ipv6 address** *IPIPV6-PREFIX/PREFIX-LENGTH* **eui-64**
- **no ipv6 address** *IPIPV6-PREFIX/PREFIX-LENGTH* **eui-64**

Parameters

Parameters	Description
IPV6-PREFIX	Specified the IPv6 prefix part for the configured IPv6 address.
PREFIX-LENGTH	Specifies the length of the prefix. The prefix of the IPv6 address is also a local subnet on the interface. The prefix length must be smaller than 64.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level：12

Usage Guideline

If the command is configured on an IPv6 ISRAP tunnel, the last 32bits of the interface ID are constructed using the source IPv4 address of the tunnel.

Example

This example shows hoe to add an IPv6 address incidence.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface vlan1
GA-MLxxTPoE+(config-if)# ipv6 address 3ffe:501:ffff:0::/64 eui-64
GA-MLxxTPoE+(config-if)#
```

7.2.5 ipv6 address dhcp

This command is used to configure an interface using DHCPv6 to get an IPv6 address. Use the **no** form of this command to disable the using of DHCPv6 to get an IPv6 address.

Syntax

ipv6 address dhcp [rapid-commit]

no ipv6 address dhcp

Parameters

Parameters	Description
rapid-commit	(Optional) Specifies to use a two-message exchange instead of the standard four-message exchange between the Requesting Router (RR) and the Delegating Router (DR) to obtain the network configuration settings from the DHCP Server.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level：12

Usage Guideline

Use this command to configure the interface to obtain IPv6 network configuration settings from a DHCPv6 server.

The standard four-message exchange between the DR and the RR includes four messages: SOLICIT, ADVERTISE, REQUEST, and REPLY. When the rapid-commit parameter is specified, the RR will notify the DR in the SOLICIT message that it can skip receiving the ADVERTISE message and sending REQUEST message, and proceed directly with receiving the REPLY message from DR to complete a two-message exchange instead of the standard four-message exchange. The REPLY message contains the network configuration settings.
The rapid-commit parameter must be enabled on both the DR and the RR to function properly.
When the no command is used, the existing IPv6 network configuration settings which are obtained from the DHCPv6 server will be removed.

Example

This example shows how to configure VLAN 1 to use DHCPv6 to get an IPv6 address.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface vlan1
GA-MLxxTPoE+(config-if)# ipv6 address dhcp
GA-MLxxTPoE+(config-if)#
```

7.2.6 ipv6 enable

This command is used to enable IPv6 processing on interfaces that have no IPv6 address explicitly configured. Use the **no** form of this command to disable IPv6 processing on interfaces that have no IPv6 address explicitly configured.

Syntax

ipv6 enable

no ipv6 enable

Parameters

None

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level：12

Usage Guideline

When the IPv6 address is explicitly configured on the interface, the IPv6 link-local address is automatically generated and the IPv6 processing is started. When the interface has no IPv6 address explicitly configured, the IPv6 link-local address is not generated and the IPv6 processing is not started. Use the **ipv6 enable command** to auto-generate the IPv6 link-local address and start the IPv6 processing on the interface.

Example

This example shows how to enable IPv6 on interface VLAN 1, which has no IPv6 address explicitly configured.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface vlan1
GA-MLxxTPoE+(config-if)# ipv6 enable
GA-MLxxTPoE+(config-if)#
```

7.2.7 ipv6 nd ns-interval

This command is used to specify the interval between retransmissions of NS messages. Use the **no** form of this command to revert to the default setting.

Syntax

- **ipv6 nd ns-interval** *MILLI-SECONDS*

  no ipv6 nd ns-interval

Parameters

Parameters	Description
MILLI-SECONDS	Specifies the amount of time between retransmissions of NS message in milliseconds. This value must be between 0 and 4294967295 milliseconds, in multiples of 1000.

Default

The default value advertised in RA is 0.
The default value used by the router is 1000 (one second).

Command Mode

Interface Configuration Mode

Command Default Level

Level：12

Usage Guideline

The configured time is used by the router on the interface and is also advertised in the RA message. If the specified time is 0, the router will use 1 second on the interface and advertise 0 (unspecified) in the RA message.

Example

This example shows how to configure the IPv6 NS message retransmission interval to 6 secondscc

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface vlan1
GA-MLxxTPoE+(config-if)# ipv6 nd ns-interval 6000
GA-MLxxTPoE+(config-if)#
```

7.2.8 ipv6 neighbor

This command is used to create a static ipv6 neighbor entry. Use the **no** form of this command to delete a IPv6 neighbor entry

Syntax

- **ipv6 neighbor** *IPV6-ADDRESS INTERFACE-ID MAC-ADDRESS*
- **no ipv6 neighbor** *IPV6-ADDRESS INTERFACE-ID*

Parameters

Parameters	Description
IPV6-ADDRESS	Specifies the IPv6 address of the IPv6 neighbor cache entry
INTERFACE-ID	Specifies the interface for creating the static IPv6 neighbor cache entry.
MAC-ADDRESS	Specifies the MAC address of the IPv6 neighbor cache entry.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level：12

Usage Guideline

Use this command to create a static IPv6 neighbor cache entry on an interface. The reachable detection process will not be applied to the static entries.

The **Clear ipv6 neighbors** command will clear the dynamic neighbor cache entries. Use the **no ipv6 neighbor** command to delete a neighbor entry.

Example

This example shows how to create a static ipv6 neighbor cache entry.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ipv6 neighbor fe80::1 vlan1 00-50-40-11-22-99
GA-MLxxTPoE+(config)#
```

7.2.9 show ipv6 general-prefix

This command is used to display IPv6 general prefix information.

Syntax

show ipv6 general-prefix [*PREFIX-NAME*]

Parameters

Parameters	Description
PREFIX-NAME	(Optional) Specifies the name of the general prefix to be displayed. If the general prefix name is not specified, all general prefixes will be displayed. The general prefix name can be up to 12 characters.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level：1

Usage Guideline

Use this command to display information of IPv6 general prefixes.

Example

This example shows how to display all IPv6 general prefix on the system.

```
GA-MLxxTPoE+#show ipv6 general-prefix

IPv6 Prefix dhcp-prefix
 Acquired via Unassigned
  Apply to interfaces
   vlan1: 1:2:3:4:5::3/64

Total Entries: 1

GA-MLxxTPoE+#
```

7.2.10 show ipv6 interface

This command is used to display IPv6 interface information.

Syntax

- **show ipv6 interface [***INTERFACE-ID***] [brief]**

Parameters

Parameters	Description
INTERFACE-ID	(Optional) Specifies the interface for display.
brief	(Optional) Specifies to display brief information.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level：1

Usage Guideline

Use this command to display IPv6 interface related configurations.

Example

This example shows how to display IPv6 interface information.

```
GA-MLxxTPoE+#show ipv6 interface vlan 1

vlan1 is up, Link status is up
 IPv6 is enabled,
 link-local address:
     FE80::250:40FF:FE3F:541B
 Global unicast address:
     3FFE:22:33:44::55/64 (Manual)
 NS messages retransmit interval is 0 milliseconds

Total Entries: 1

GA-MLxxTPoE+#
```

This example shows how to display brief IPv6 interface information.

```
GA-MLxxTPoE+#show ipv6 interface brief

vlan1 is up, Link status is up
    FE80::250:40FF:FE3F:541B
    3FFE:22:33:44::55


Total Entries: 1

GA-MLxxTPoE+#
```

7.2.11 show ipv6 neighbors

This command is used to display IPv6 neighbor information.

構文

- **show ipv6 neighbors [***INTERFACE-ID* **] [***IPV6-ADDRESS* **]**

Parameters

Parameters	Description
INTERFACE-ID	(option) Specifies the interface to display IPv6 neighbor cache entry.
IPV6-ADDRESS	(option) Specifies the IPv6 address to display its IPv6 neighbor cache entry.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level：1

Usage Guideline

Use this command to display the IPv6 neighbor cache entry.

Example

This example shows how to display the IPv6 neighbor cache entry.

```
GA-MLxxTPoE+# show ipv6 neighbors

IPv6 Address                          Link-Layer Addr   Interface Type State
------------------------------------- ----------------- --------- ---- -----
FE80::200:11FF:FE22:3344              00-50-40-22-33-44 vlan1     D    REACH

Total Entries: 1

GA-MLxxTPoE+#
```

Display Parameters

Parameters	Description
Type	D - Dynamic learning entry. S - Static neighbor entry.

Parameters	Description
State	INCMP (Incomplete) - Address resolution is being performed on the entry, but the corresponding neighbor advertisement message has not yet been received. REACH (Reachable) - Corresponding neighbor advertisement message was received and the reachable time (in milliseconds) has not elapsed yet. It indicates that the neighbor was functioning properly. STALE - More than the reachable time (in milliseconds) have elapsed since the last confirmation was received. PROBE - Sending the neighbor solicitation message to confirm the reachability. DELAY - The neighbor is no longer known to be reachable and traffic has recently been sent to the neighbor. Instead of probing the neighbor immediately, delay the sending of probes for a short while in order to give upper-layer protocols a chance to provide reachability confirmation.

7.3 ARP Refresh Commands

7.3.1 arp refresh before-time-out

This command is used to enable the sending of ARP packets before ARP timeout. Use the **no** form of this command to disable the function.

Syntax

arp refresh before-time-out

no arp refresh before-time-out

Parameters

None

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode

Command Default Level

Level：15

Usage Guideline

Use this command to enable the sending of ARP packets before ARP timeout.

実行例

This example shows how to enable the sending of ARP packets before ARP timeout.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#arp refresh before-time-out
GA-MLxxTPoE+(config)#
```

7.3.2 show arp refresh before-time-out

This command is used to display the status of the ARP refresh before timeout.

Syntax

show arp refresh before-time-out

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level : 1

Usage Guideline

Use this command to display the status of the ARP refresh before timeout.

Example

This example shows how to display the status of the ARP refresh before timeout.

```
GA-MLxxTPoE+#show arp refresh before-time-out

Arp refresh timeout state is : Enabled


GA-MLxxTPoE+#
```

7.4 Gratuitous ARP Commands

7.4.1 ip arp gratuitous

This command is used to enable the learning of gratuitous ARP packets in the ARP cache table. Use the **no** form of this command to disable ARP control.

Syntax

- **ip arp gratuitous**
- **no ip arp gratuitous**

Parameters

None

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12

Usage Guideline

The system will learn gratuitous ARP packets in the ARP cache table by default.

Example

This example shows how to disable the learning of gratuitous ARP request packets.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# no ip arp gratuitous
GA-MLxxTPoE+(config)#
```

7.4.2 ip gratuitous-arps

This command is used to enable the transmission of gratuitous ARP request packets. Use the **no** form of this command to disable the transmission.

Syntax

- **ip gratuitous-arps [dad-reply]**
- **no ip gratuitous-arps [dad-reply]**

Parameters

Parameters	Description
dad-reply	(Optional) Specifies control whether the system will reply with another gratuitous ARP request packet with the broadcast DA, when receiving a gratuitous ARP request packet and detecting the duplicate IP address.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

A gratuitous ARP request packet is an ARP request packet where the source and the destination IP address are both set to the IP address of the sending device and the destination MAC address is the broadcast address.
Generally, a device use the gratuitous ARP request packet to discover whether the IP address is duplicated by other hosts or to preload or reconfigure the ARP cache entry of hosts connected to the interface.
Use the **ip gratuitous-arps** command to enable transmission of gratuitous ARP request. The device will send out the packet when an IP interface becomes link-up or when the IP address of an interface is configured or modified.

Use the **ip gratuitous-arps dad-reply** command to enable the transmission of gratuitous ARP requests. The device will send out the packet while a duplicate IP address is detected

Example

This example shows how to sending of gratuitous ARP messages.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip gratuitous-arps dad-reply
GA-MLxxTPoE+(config)#
```

7.4.3 arp gratuitous-send interval

This command is used to set the interval for regularly sending of gratuitous ARP request messages on the interface. Use the **no** form of this command to disable this function on the interface.

Syntax

- **arp gratuitous-send interval** *SECONDS*
- **no arp gratuitous-send**

Parameters

Parameters	Description
SECONDS	Specifies the time interval to send the gratuitous ARP request message. The value is from 0 to 3600. 0 represents that this option is disabled.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

If an interface on the Switch is used as the gateway of its downlink devices and counterfeit gateway behavior occurs in the downlink devices, administrators can configure to send gratuitous ARP request messages regularly on this interface to notify that the Switch is the real gateway.

Example

This example shows how to enable the sending of gratuitous ARP messages.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#ip gratuitous-arps
GA-MLxxTPoE+(config)#interface vlan 1
GA-MLxxTPoE+(config-if)#arp gratuitous-send interval 1
GA-MLxxTPoE+(config-if)#
```

7.4.4 snmp-server enable traps gratuitous-arp

This command is used to enable the sending of SNMP notifications for gratuitous ARP duplicate IP detected. Use the **no** form of this command to disable the function.

Syntax

- **snmp-server enable traps gratuitous-arp**
- **no snmp-server enable traps gratuitous-arp**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to enable or disable the sending of SNMP notifications for gratuitous ARP duplicate IP detected.

Example

This example shows how to enable the sending of SNMP notifications for gratuitous ARP duplicate IP detected.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#snmp-server enable traps gratuitous-arp
GA-MLxxTPoE+(config)#
```

7.5 Dynamic ARP Inspection Commands

7.5.1 arp access-list

This command is used to create or modify an ARP access list. This command will enter into the ARP access-list configuration mode. Use the **no** form of this command to remove an ARP access-list.

Syntax

- **arp access-list** *NAME*
- **no arp access-list** *NAME*

Parameters

Parameters	Description
NAME	Specifies the name of the ARP access-list to be configured. The maximum length is 32 characters.

Default

None

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12

Usage Guideline

The name must be unique among all access-lists. The characters used in the name are case sensitive. There is an implicit deny statement at the end of an access list.

Example

This example shows how to configure an ARP access list with two permit entries.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# arp access-list static-arp-list
GA-MLxxTPoE+(config-arp-nacl)# permit ip 10.20.0.0 0.0.255.255 mac any
GA-MLxxTPoE+(config-arp-nacl)# permit ip 10.30.0.0 0.0.255.255 mac any
GA-MLxxTPoE+(config-arp-nacl)#
```

7.5.2 clear ip arp inspection log

This command is used to clear the ARP inspection log buffer.

Syntax

- clear ip arp inspection log

Parameters

None

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to clear the ARP inspection log buffer.

Example

This example shows how to clear the inspection log.

```
GA-MLxxTPoE+# clear ip arp inspection log
GA-MLxxTPoE+#
```

7.5.3 clear ip arp inspection statistics

This command is used to clear the dynamic ARP inspection statistics.

Syntax

- **clear ip arp inspection statistics** {**all** | **vlan** *VLAN-ID* [**,** | **-**]}

Parameters

Parameters	Description
all	Specifies to clear dynamic ARP inspection statistics from all VLANs.
vlan *VLAN-ID*	Specifies the VLAN or range of VLANs.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to clear the Dynamic ARP Inspection (DAI) statistics.

Example

This example shows how to clear the DAI statistics from VLAN 1.

```
GA-MLxxTPoE+# clear ip arp inspection statistics vlan 1
GA-MLxxTPoE+#
```

7.5.4 ip arp inspection filter vlan

This command is used to specify an ARP access list to be used for ARP inspection checks for the VLAN. Use the **no** command to remove the specification.

Syntax

- **ip arp inspection filter** *ARP-ACL-NAME* **vlan** *VLAN-ID* [**,** | **-**] [**static**]
- **no ip arp inspection filter** *ARP-ACL-NAME* **vlan** *VLAN-ID* [**,** | **-**] [**static**]

Parameters

Parameters	Description
ARP-ACL-NAME	Specifies the access control list name with a maximum of 32 characters.
vlan *VLAN-ID*	Specifies the VLAN associated with the ARP access list.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.
static	(Optional) Specifies to drop the packet if the IP-to-Ethernet MAC binding pair is not permitted by the ARP ACL.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to specify an ARP access list to be used for ARP inspection checks for the VLAN. Up to one access list can be specified for a VLAN.

The dynamic ARP inspection checks the ARP packets received on the VLAN to verify that the binding pair of the source IP and source MAC address of the packet is valid. The validation process will match the address binging against the entries of the DHCP snooping database. If the command is configured, the validation process will match the address binging against the access list entries and the DHCP snooping database.
ARP ACLs take precedence over entries in the DHCP snooping binding database. If the packet is explicitly denied by the access control list, the packet is dropped. If the packet is denied due to the implicit deny, the packet will be further matched against the DHCP snooping binding entries if the keyword “static” is not specified. The implicit denied packet is dropped if the keyword “static” is specified.

Example

This example shows how to apply the ARP ACL static ARP list to VLAN 10 for DAI.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip arp inspection filter static-arp-list vlan 10
GA-MLxxTPoE+(config)#
```

7.5.5 ip arp inspection limit

This command is used to limit the rate of incoming ARP requests and responses on an interface. Use the **no** form of this command to revert to the default settings.

Syntax

- **ip arp inspection limit {rate** *VALUE* **[burst interval** *SECONDS*] **| none}**
- **no ip arp inspection limit**

Parameters

Parameters	Description
rate *VALUE*	Specifies the maximum number per second of the ARP packets that can be processed. The valid range is from 1 to 150 seconds.
burst interval *SECONDS*	(Optional) Specifies the length of the burst duration of the ARP packets that is allowed. The valid range is from 1 to 15. If not specified, the default setting is one second.
none	Specifies that there is no limit on the ARP packet rate.

Default

For DAI untrusted interfaces, the rate limit is 15 packets per second with a burst interval of 1 second.
For DAI trusted interfaces, the rate has no limit.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command takes effect for both trusted and un-trusted interfaces. When the rate of the ARP packet per second exceeds the limitation and the condition sustained for the configured burst duration, the port will be put in the error disable state.

Example

This example shows how to limit the rate of the incoming ARP requests to 30 packets per second and to set the interface monitoring interval to 5 consecutive seconds.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/10
GA-MLxxTPoE+(config-if)# ip arp inspection limit rate 30 burst interval 5
GA-MLxxTPoE+(config-if)#
```

7.5.6 ip arp inspection log-buffer

This command is used to configure the ARP inspection log buffer parameter.

Syntax

- **ip arp inspection log-buffer entries** *NUMBER*
- **no ip arp inspection log-buffer entries**

Parameters

Parameters	Description
NUMBER	Specifies the buffer entry number. The maximum number is 1024.

Default

By default, this value is 32.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use the command to configure the maximum entry number of the log buffer. The ARP inspection log buffer keeps tracks the information of ARP packet. The first packet that is given by check will be sent to syslog module and recorded in the inspection log buffer. The subsequent packets belonging to the same session will not be sent to log module unless its record in the log buffer is cleared. If the log buffer is full but more logging events, the event will not be logged. If the user specifies a buffer size less than the current entry number, then the log buffer will be automatically cleared.

Example

This example shows how to change the maximum buffer number to 64.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip arp inspection log-buffer entries 64
GA-MLxxTPoE+(config)#
```

7.5.7 ip arp inspection trust

This command is used to trust an interface for dynamic ARP inspection. Use the **no** form of this command to disable the trust state.

Syntax

- **ip arp inspection trust**
- **no ip arp inspection trust**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

When an interface is in the trust state, the ARP packets arriving at the interface will not be inspected. When an interface is in the untrusted state, ARP packets arriving at the port and belongs to the VLAN that is enabled for inspection will be inspected.

Example

This example shows how to configure GigabitEthernet1/0/3 to be trusted for DAI.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/3
GA-MLxxTPoE+(config-if)# ip arp inspection trust
GA-MLxxTPoE+(config-if)#
```

7.5.8 ip arp inspection validate

This command is used to specify the additional checks to be performed during an ARP inspection check. Use the **no** form of this command to remove specific additional check.

Syntax

- **ip arp inspection validate [src-mac] [dst-mac] [ip]**
- **no ip arp inspection validate [src-mac] [dst-mac] [ip]**

Parameters

Parameters	Description
src-mac	(Optional) Specifies to check for ARP requests and response packets and the consistency of the source MAC address in the Ethernet header against the sender MAC address in the ARP payload.
dst-mac	(Optional) Specifies to check for ARP response packets and the consistency of the destination MAC address in the Ethernet header against the target MAC address in the ARP payload.
ip	(Optional) Specifies to check the ARP body for invalid and unexpected IP addresses. Specifies to check the validity of IP address in the ARP payload. The sender IP in both the ARP request and response and target IP in the ARP response are validated. Packets destined for the IP addresses 0.0.0.0, 255.255.255.255, and all IP multicast addresses are dropped. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to specify the additional checks to be performed during the dynamic ARP inspection check. The specified check will be performed on packets arriving at the untrusted interface and belong to the VLANs that are enabled for IP ARP inspection. If no parameters are specified, all options are enabled or disabled. Use the **no** form of the command with the specific option to disable the specific type of check.

Example

This example shows how to enable source MAC validation.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip arp inspection validate src-mac
GA-MLxxTPoE+(config)#
```

7.5.9 ip arp inspection vlan

This command is used to enable specific VLANs for dynamic ARP inspection. Use the **no** form of this command to disable dynamic ARP inspection for VLAN.

Syntax

- **ip arp inspection vlan** *VLAN-ID* [**,** | **-**]
- **no ip arp inspection vlan** *VLAN-ID* [**,** | **-**]

Parameters

Parameters	Description
VLAN-ID	Specifies the VLAN to enable or disable the ARP inspection function.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.

Default

By default, ARP inspection is disabled on all VLANs.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

When a VLAN is enabled for ARP inspection, the ARP packets, including both the ARP request and response packet belonging to the VLAN arriving at the untrusted interface will be validated. If the IP-to-MAC address binding pair of the source MAC address and the source IP address is not permitted by the ARP ACL or the DHCP snooping binding database, the ARP packet will be dropped. In addition to the address binding check, the additional check defined by the IP ARP inspection validate command will also be checked.

Example

This example shows how to enable ARP inspection on VLAN 2.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip arp inspection vlan 2
GA-MLxxTPoE+(config)#
```

7.5.10 ip arp inspection vlan logging

This command is used to control the type of packets that are logged. Use the **no** form of this command to revert to the default settings.

Syntax

- **ip arp inspection vlan** *VLAN-ID* **[, | -] logging {acl-match {permit | all | none} | dhcp-bindings {permit | all | none}}**
- **no ip arp inspection vlan** *VLAN-ID* **[, | -] logging {acl-match | dhcp-bindings}**

Parameters

Parameters	Description
VLAN-ID	Specifies the VLAN to enable or disable the logging control function.

Parameters	Description
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.
acl-match	Specifies the logging criteria for packets that are dropped or permitted based on ACL matches.
permit	Specifies logging when permitted by the configured ACL.
all	Specifies logging when permitted or denied by the configured ACL.
none	Specifies that ACL-matched packets are not logged.
dhcp-bindings	Specifies the logging criteria for packets dropped or permitted based on matches against the DHCP bindings.
permit	Specifies logging when permitted by DHCP bindings.
all	Specifies logging when permitted or denied by DHCP bindings.
none	Specifies to prevent the logging of all packets permitted or denied by DHCP bindings.

Default

All denied or dropped packets are logged.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use the no form of this command to reset some of the logging criteria to their defaults.

Example

This example shows how to configure an ARP inspection on VLAN 1 to add packets to a log that matches the ACLs.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip arp inspection vlan 1 logging acl-match all
GA-MLxxTPoE+(config)#
```

7.5.11 permit | deny (arp access-list)

This command is used to define the ARP permit entry. Use the **deny** command to define the ARP deny entry. Use the **no** form of this command to remove an entry

Syntax

- {**permit** | **deny**} **ip** {**any** | **host** *SENDER-IP* | *SENDER-IP SENDER-IP-MASK*} **mac** {**any** | **host** *SENDER-MAC* | *SENDER-MAC SENDER-MAC-MASK*}
- **no** {**permit** | **deny**} **ip** {**any** | **host** *SENDER-IP* | *SENDER-IP SENDER-IP-MASK*} **mac** {**any** | **host** *SENDER-MAC* | *SENDER-MAC SENDER-MAC-MASK*}

Parameters

Parameters	Description
ip	Specifies the source IP address.
any	Specifies to match any source IP address.
host *SENDER-IP*	Specifies to match a single source IP address.
SENDER-IP SENDER-IP-MASK	Specifies to match a group of source IP addresses by using a bitmap mask. The bit corresponding to bit value 1 will be checked. The input format is the same as IP address.
mac	Specifies the MAC address.
any	Specifies to match any source MAC address.
host *SENDER-MAC*	Specifies to match a single source MAC address.
SENDER-MAC SENDER-MAC-MASK	Specifies to match a group of source MAC addresses by using a bitmap mask. The bit corresponding to bit value 1 will be checked. The input format is the same as MAC address.

Default

None

Command Mode

ARP Access-list Configuration Mode.

Command Default Level

Level: 12

Usage Guideline

Using the **permit any** option will permit the rest of the packets that do not match any previous rule.

Example

This example shows how to configure an ARP access-list with two permit entries.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# arp access-list static-arp-list
GA-MLxxTPoE+(config-arp-nacl)# permit ip 10.20.0.0 255.255.0.0 mac any
GA-MLxxTPoE+(config-arp-nacl)# permit ip 10.30.0.0 255.255.0.0 mac any
GA-MLxxTPoE+(config-arp-nacl)#
```

7.5.12 show ip arp inspection

This command is used to display the status of DAI for a specific range of VLANs.

Syntax

- **show ip arp inspection** [**interfaces** [*INTERFACE-ID* [**,** | **-**]] | **statistics** [**vlan** *VLAN-ID* [**,** | **-**]]]

Parameters

Parameters	Description
interfaces *INTERFACE-ID*	(Optional) Specifies a port, range of ports or all ports to configure.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
statistics	(Optional) Specifies the DAI statistics.
vlan *VLAN-ID*	(Optional) Specifies a VLAN or range of VLANs.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.

Default

None

Command Mode

User EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command is used to display the status of DAI for a specific range of VLANs.

Example

This example shows how to display the statistics of packets that have been processed by DAI for VLAN 10.

```
GA-MLxxTPoE+#show ip arp inspection statistics vlan 1

VLAN Forwarded Dropped DHCPDrops ACL Drops
---- --------- ------- --------- ---------
1    21546     145261  145261    0
VLAN DHCP Permits ACL Permits Source MAC Failures
---- ------------ ------------ -------------------
1    21546        0            0
VLAN Dest MAC Failures IP Validation Failures
---- ----------------- ----------------------
1     0                 0

GA-MLxxTPoE+#
```

This example shows how to display the statistics of packets that have been processed by DAI for all active VLANs.

```
GA-MLxxTPoE+# show ip arp inspection statistics

VLAN    Forwarded    Dropped    DHCP Drops   ACL Drops
-----   ---------   ---------   ----------   ---------
1       0           0           0            0
2       0           0           0            0
10      21546       145261      145261       0
100     0           0           0            0
200     0           0           0            0
1024    0           0           0            0
VLAN    DHCP Permits   ACL Permits   Source MAC Failures
-----   ------------   -----------   -------------------
1       0              0             0
2       0              0             0
10      21546          0             0
100     0              0             0
200     0              0             0
1024    0              0             0
VLAN    Dest MAC Failures   IP Validation Failures
-----   -----------------   ----------------------
1        0                        0
2        0                        0
10       0                        0
100      0                        0
200      0                        0
1024     0                        0

GA-MLxxTPoE+#
```

Display Parameters

Parameters	Description
VLAN	The VLAN ID that is enabled for ARP inspection.
Forwarded	The number of ARP packets that are forwarded by ARP inspection.
Dropped	The number of ARP packets that are dropped by ARP inspection.
DHCP Drops	The number of ARP packets that are dropped by DHCP snooping binding database.
ACL Drops	The number of ARP packets that are dropped by ARP ACL rule.
DHCP Permits	The number of ARP packets that are permitted by DHCP snooping binding database.
ACL Permits	The number of ARP packets that are permitted by ARP ACL rule.
Source MAC Failures	The number of ARP packets that fail source MAC validation.
Dest MAC Failures	The number of ARP packets that fail destination MAC validation.

Parameters	Description
IP Validation Failures	The number of ARP packets that fail the IP address validation.

Example

This example shows how to display the configuration and operating state of DAI.

```
GA-MLxxTPoE+#show ip arp inspection

Source MAC Validation     : Enabled
Destination MAC Validation: Disabled
IP Address Validation     : Disabled
VLAN State    ACL Match                         Static ACL
---- -------- --------------------------------- ----------
10   Disabled static-arp-list                   No
VLAN ACL Logging DHCP Logging
---- ----------- ------------
10   Deny        Deny

GA-MLxxTPoE+#
```

Display Parameters

Parameters	Description
VLAN	The VLAN ID that enables ARP inspection.
State	The configuration state of ARP inspection. **Enabled:** ARP inspection is enabled. **Disabled:** ARP inspection is enabled.
ACL Match	The name of ARP ACL that is specified.
Static ACL	The configuration of the static ACL. **Yes:** Static ARP ACL is configured. **No:** Static ARP ACL is not configured.
ACL logging	The state of logging for packets dropped or permitted based on ACL matches. **None:** ACL-matched packets are not logged. **Permit:** Logging when packets are permitted by the configured ACL. **Deny:** Logging when packets are dropped by the configured ACL. **All:** ACL-matched packets are always logged.

Parameters	Description
DHCP Logging	The state of logging for packets dropped or permitted based on DHCP bindings. **None:** Prevent logging when packets are dropped or permitted by the DHCP bindings. **Permit:** Logging when packets are permitted by the DHCP bindings. **Deny:** Logging when packets are dropped by the DHCP bindings. **All:** Logging when packets are dropped or permitted by the DHCP bindings.

Example

This example shows how to display the trust state of GigabitEthernet1/0/10.

```
GA-MLxxTPoE+#show ip arp inspection interfaces gi1/0/10

Interface       Trust State Rate(pps) Burst Interval
--------------- ----------- --------- --------------
Gi1/0/10        trusted     None      1
Total Entries: 1

GA-MLxxTPoE+#
```

This example shows how to display the trust state of interfaces on the Switch.

```
GA-MLxxTPoE+#show ip arp inspection interfaces

Interface       Trust State Rate(pps) Burst Interval
--------------- ----------- --------- --------------
Gi1/0/1         untrusted   15        1
Gi1/0/2         untrusted   15        1
Gi1/0/3         untrusted   15        1
Gi1/0/4         untrusted   15        1
Gi1/0/5         untrusted   15        1
Gi1/0/6         untrusted   15        1
Gi1/0/7         untrusted   15        1
Gi1/0/8         untrusted   15        1
Gi1/0/9         untrusted   15        1
Gi1/0/10        trusted     None      1
Gi1/0/11        untrusted   15        1
Gi1/0/12        untrusted   15        1
Gi1/0/13        untrusted   15        1
Gi1/0/14        untrusted   15        1
Gi1/0/15        untrusted   15        1
Gi1/0/16        untrusted   15        1
Gi1/0/17        untrusted   15        1
Gi1/0/18        untrusted   15        1
Gi1/0/19        untrusted   15        1
Gi1/0/20        untrusted   15        1
Gi1/0/21        untrusted   15        1
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

Display Parameters

Parameters	Description
Interface	The name of interface that enable ARP inspection.
Trust State	The state of the interface. **trusted:** This interface is ARP inspection trusted port, all ARP packet will be legal and not be authorized. **untrusted:** This interface is ARP inspection untrusted port, all ARP packet will be authorized.
Rate (pps)	The upper limit on the number of incoming packets processed per second.
Burst Interval	The consecutive interval in seconds over which the interface is monitored for the high rate of the ARP packets.

7.5.13 show ip arp inspection log

This command is used to display the ARP inspection log buffer.

Syntax

- show ip arp inspection log

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display the content of the inspection log buffer.

Example

This example shows how to display the inspection log-buffer.

```
GA-MLxxTPoE+#show ip arp inspection log
Total log buffer size: 64

Interface       VLAN Sender IP       Sender MAC        Occurrence
--------------- ---- --------------- ----------------- ------------------------
Gi1/0/1         100  10.20.1.1       00-20-30-40-50-60 1 (2013-12-28 23:08:66)
Gi1/0/2         100  10.5.10.16      55-66-20-30-40-50 2 (2013-12-02 00:11:54)
Gi1/0/3         100  10.58.2.30      10-22-33-44-50-60 1 (2013-12-30 12:01:38)

Total Entries: 3

GA-MLxxTPoE+#
```

Display Parameters

Parameters	Description
Interface	The name of interface that logging occurred.
VLAN	The VLAN that logging occurred.
Sender IP	The logging ARP's sender IP address.
Sender MAC	The logging ARP's sender MAC address.
Occurrence	The counter of logging entries occurred and the last time of logging entry occurred.

7.6 IP Setup Interface commands

7.6.1 ip setup interface

This command is used to enable the IP setup interface function. Use the **no** form of this command to disable the function.

Syntax

- **ip setup interface**

  no ip setup interface

Parameters

None

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level：12

Usage Guideline

The command is used to enable or disable the IP setup interface function.

Example

This example shows how to enable IP setup interface.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#ip setup interface
GA-MLxxTPoE+(config)#
```

7.6.2 show ip_setup_interface

This command is used to display the IP setup interface status.

Syntax

- **show ip_setup_interface**

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level：1

Usage Guideline

This command is used to display the IP setup interface status.

Example

This example shows how to display the IP setup interface status.

```
GA-MLxxTPoE+#show ip_setup_interface
IP Setup Interface: Enabled

GA-MLxxTPoE+#
```

8 Multicast Control

8.1 IGMP (Internet Group Management Protocol) Snooping Commands

IGMP (Internet Group Management Protocol) is a protocol to manage multicast groups. IGMP snooping is a filtering function to monitor IGMP packets flowing on ports of the switch and prevent data from flowing to unnecessary ports. This filtering function allows to efficiently process a large amount of data, such as video distribution.

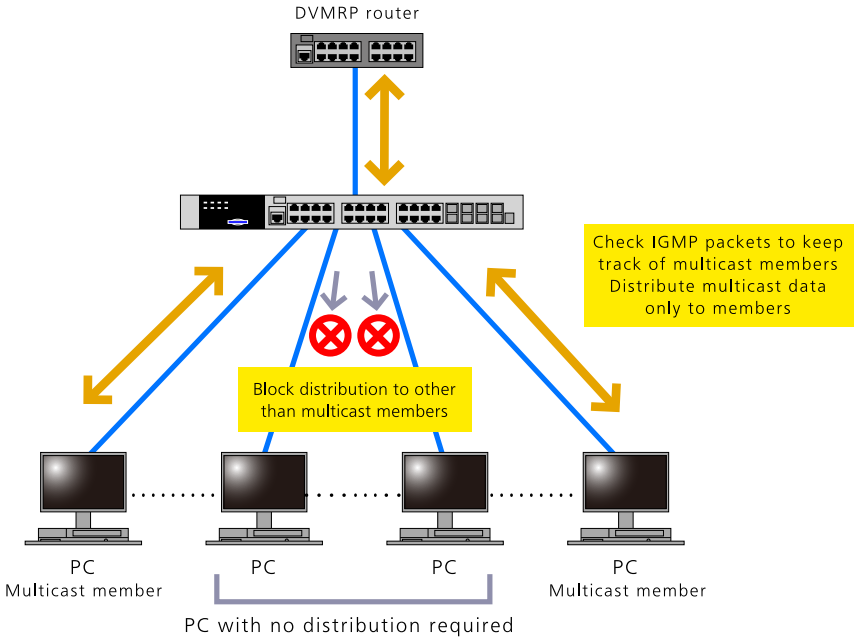


Figure 55-1 IGMP Snooping overview

8.1.1 clear ip igmp snooping statistics

This command is used to clear the IGMP snooping related statistics.

Syntax

- **clear ip igmp snooping statistics** {**all** | **vlan** *VLAN-ID* | **interface** *INTERFACE-ID*}

Parameters

Parameters	Description
all	Specifies to clear IP IGMP snooping statistics for all VLANs and all ports.
vlan *VLAN-ID*	Specifies a VLAN to clear the IP IGMP snooping statistics.
interface *INTERFACE-ID*	Specifies a port to clear the IP IGMP snooping statistics.

Default

None

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12

Usage Guideline

This command is used to clear the IGMP snooping related statistics.

Example

This example shows how to clear all IGMP Snooping statistics.

```
GA-MLxxTPoE+# clear ip igmp snooping statistics all
GA-MLxxTPoE+#
```

8.1.2 ip igmp snooping

This command is used to enable the IGMP snooping function on the Switch. Use the **no** form of this command to disable the IGMP snooping function.

Syntax

- **ip igmp snooping**
- **no ip igmp snooping**

Parameters

None

Default

IGMP snooping is disabled on all VLAN interfaces.
The IGMP snooping global state is disabled.

Command Mode

Interface Configuration Mode
Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

In the interface configuration mode, the command is only available for VLAN interface configuration. For a VLAN to operate with IGMP snooping, both the global state and per interface state must be enabled. On a VLAN, the setting of IGMP snooping and MLD snooping are independent. IGMP snooping and MLD snooping can be simultaneously enabled on the same VLAN.

Example

This example shows how to disable the IGMP snooping operation on all VLANs.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# no ip igmp snooping
GA-MLxxTPoE+(config)#
```

This example shows how to enable the IGMP snooping operation on all VLANs.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip igmp snooping
GA-MLxxTPoE+(config)#
```

This example shows how to disable IGMP snooping on VLAN 1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1
GA-MLxxTPoE+(config-vlan)# no ip igmp snooping
GA-MLxxTPoE+(config-vlan)#
```

8.1.3 ip igmp snooping access-group

This command is used to restrict the receivers on a subnet to only join the multicast groups that are permitted by a standard IP access list. Use the **no** form of this command to disable this function.

Syntax

- **ip igmp snooping access-group** *ACCESS-LIST-NAME* [**vlan** *VLAN-ID*]
- **no ip igmp snooping access-group** [**vlan** *VLAN-ID*]

Parameters

Parameters	Description
ACCESS-LIST-NAME	Specifies a standard IP access list. To permit users to join a group (*, G), specify "any" in source address field and G in destination address field of the access list entry.
vlan *VLAN-ID*	(Optional) Specifies a Layer 2 VLAN on a trunk port and applies the filter to packets arrive on that VLAN.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use the **ip igmp snooping access-group** command on the Switch to restrict the multicast traffic receiver to join to specific group. The destination address part of the access list represents the multicast group address that the receiver is permitted or denied to join.
This command is available for physical port or port-channel interface configuration.

Example

This example shows how to restrict the serviced IGMP snooping group for GigabitEthernet1/0/1 to group 226.1.1.1. In the following example, first, create an IP access list named “igmp_filter” which only permits the packets destined for group address 226.1.1.1. Then, associate this access group in GigabitEthernet1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip access-list igmp_filter
GA-MLxxTPoE+(config-ip-acl)# permit any host 226.1.1.1
GA-MLxxTPoE+(config-ip-acl)# end
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# ip igmp snooping access-group igmp_filter
GA-MLxxTPoE+(config-if)#
```

8.1.4 ip igmp snooping fast-leave

This command is used to configure IGMP Snooping fast-leave on the interface. Use the no form of this command to disable the fast-leave option on the specified interface.

Syntax

- ip igmp snooping fast-leave
- no ip igmp snooping fast-leave

Parameters

None

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command is only available for VLAN interface configuration. The **ip igmp snooping fast-leave** command allows IGMP membership to be removed from a port right on receiving the leave message without using the group specific or group-source specific query mechanism.

Example

This example shows how to enable IGMP snooping fast-leave on VLAN 1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1
GA-MLxxTPoE+(config-vlan)# ip igmp snooping fast-leave
GA-MLxxTPoE+(config-vlan)#
```

8.1.5 ip igmp snooping last-member-query-interval

This command is used to configure the interval at which the IGMP snooping querier sends IGMP group-specific or group-source-specific (channel) query messages. Use the **no** form of this command to revert to the default setting.

Syntax

- **ip igmp snooping last-member-query-interval** *SECONDS*
- **no ip igmp snooping last-member-query-interval**

Parameters

Parameters	Description
SECONDS	Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. The range of this value is 1 to 25.

Default

By default, this value is 1 second.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command is only available for VLAN interface configuration. On receiving an IGMP leave message, the IGMP snooping querier will assume that there are no local members on the interface if there are no reports received after the response time. Users can lower this interval to reduce the amount of time it takes a switch to detect the loss of the last member of a group.

Example

This example shows how to configure the last member query interval time to be 3 seconds.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1000
GA-MLxxTPoE+(config-vlan)# ip igmp snooping last-member-query-interval 3
GA-MLxxTPoE+(config-vlan)#
```

8.1.6 ip igmp snooping limit

This command is used to set the limitation on the number of IGMP cache entries that can be created. Use the **no** form of this command to remove the limitation.

Syntax

- **ip igmp snooping limit** *NUMBER* **[exceed-action {drop | replace}] [except** *ACCESS-LIST-NAME*] **[vlan** *VLAN-ID*]
- **no ip igmp snooping limit [vlan** *VLAN-ID*]

Parameters

Parameters	Descriptions
NUMBER	Specifies to set the maximum number of IGMP cache entries that can be created. This value must be between 1 and 1024.
exceed-action	(Optional) Specifies the action for handling newly learned groups when the limitation is exceeded.
drop	(Optional) Specifies that the new group will be dropped.
replace	(Optional) Specifies that the new group will replace the oldest group.

Parameters	Descriptions
except *ACCESS-LIST-NAME*	(Optional) Specifies a standard IP access list. The group (*,G), or channel (S,G) permitted by the access list will be excluded from the limit. To permit a channel (S,G), specifies S in the source address field and G in the destination address field of the access list entry. To permit a group (*,G), specifies "any" in the source address field and G in the destination address field of the access list entry.
vlan *VLAN-ID*	(Optional) Specifies a Layer 2 VLAN and applies the filter to packets that arrive on that VLAN.

Default

By default, there is no limit.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command is available for physical port or port-channel interface configuration. The except-option allows users to specify a standard access list to exclude a list of groups or channels from the limit.

Example

This example shows how to set the limit number of IGMP snooping groups with a configuration limit from an ACL that GigabitEthernet1/0/4 with the VLAN ID of 1000 can join to.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/4
GA-MLxxTPoE+(config-if)# ip igmp snooping limit 80 except igmp_filter vlan 1000
GA-MLxxTPoE+(config-if)#
```

This example shows how to reset the limit number to the default of IGMP snooping groups that port-channel 4 with the VLAN ID of 1000 can join to.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface port-channel 4
GA-MLxxTPoE+(config-if)# no ip igmp snooping limit vlan 1000
GA-MLxxTPoE+(config-if)#
```

8.1.7 ip igmp snooping mrouter

This command is used to configure the specified interface(s) as the multicast router ports or as forbidden to be multicast router ports on the Switch. Use the **no** form of this command to remove the interface(s) from router ports or forbidden multicast router ports.

Syntax

- **ip igmp snooping mrouter {interface** *INTERFACE-ID* **[, | -] | forbidden interface** *INTERFACE-ID* **[, | -]}**
- **no ip igmp snooping mrouter {interface** *INTERFACE-ID* **[, | -] | forbidden interface** *INTERFACE-ID* **[, | -]}**

Parameters

Parameters	Description
interface	Specifies a static multicast router port.
forbidden interface	Specifies a port that cannot be multicast router port.
INTERFACE-ID	Specifies an interface or an interface list. The interface can be a physical interface or a port-channel.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

No IGMP snooping multicast router port is configured.
Auto-learning is enabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for VLAN interface configuration. To specify a multicast router port, the valid interface can be a physical port or a port-channel. The specified multicast router port must be member port of the configured VLAN. A multicast router port can be either dynamic learned or statically configured. With the dynamic learning, the IGMP snooping entity will learn IGMP, PIM, or DVMRP packet to identify a multicast router port. If auto-learn is disabled, the multicast router port can only be statically configured.

Example

This example shows how to add an IGMP snooping static multicast router port for VLAN 1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1
GA-MLxxTPoE+(config-vlan)# ip igmp snooping mrouter interface gi1/0/4
GA-MLxxTPoE+(config-vlan)#
```

8.1.8 ip igmp snooping proxy-reporting

This command is used to enable the proxy-reporting function. Use the **no** form of this command to disable the proxy-reporting function.

Syntax

- **ip igmp snooping proxy-reporting** [**source** *IP-ADDRESS*]
- **no ip igmp snooping proxy-reporting**

Parameters

Parameters	Description
source *IP-ADDRESS*	(Optional) Specifies the source IP of proxy reporting. The default value is zero IP.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for VLAN interface configuration. When the function proxy reporting is enabled, the received multiple IGMP report or leave packets for a specific (S, G) will be integrated into one report before being sent to the router port. Proxy reporting source IP will be used as source IP of the report, Zero IP address will be used when the proxy reporting source IP is not set. Interface MAC will be used as source MAC of the report. If the VLAN has no IP address configured, then system MAC will be used.

Example

This example shows how to enable IGMP snooping proxy-reporting on VLAN 1 and configure the proxy-reporting message source IP to be 1.2.2.2.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1
GA-MLxxTPoE+(config-if)# ip igmp snooping proxy-reporting source 1.2.2.2
GA-MLxxTPoE+(config-if)#
```

8.1.9 ip igmp snooping querier

This command is used to enable the capability of the entity as an IGMP querier. Use the **no** form of this command to disable the querier function.

Syntax

- **ip igmp snooping querier**
- **no ip igmp snooping querier**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for VLAN interface configuration. The interface must have IP address assigned to start the querier. The system will return warning message if the VLAN has no IP address. If querier is enabled, but IP address is removed, the querier will be stopped. If the system can play the querier role, the entity will listen for IGMP query packets sent by other devices. If IGMP query message is received, the device with lower value of IP address becomes the querier. If IGMP protocol is also enabled on the interface, IGMP snooping querier state will be disabled automatically.

Example

This example shows how to enable the IGMP snooping querier on VLAN 1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1
GA-MLxxTPoE+(config-vlan)# ip igmp snooping querier
GA-MLxxTPoE+(config-vlan)#
```

8.1.10 ip igmp snooping query-interval

This command is used to configure the interval at which the IGMP snooping querier sends IGMP general query messages periodically. Use the **no** form of this command to revert to the default setting.

Syntax

- **ip igmp snooping query-interval** *SECONDS*
- **no ip igmp snooping query-interval**

Parameters

Parameters	Description
SECONDS	Specifies to configure the interval at which the designated router sends IGMP general-query messages. The range is from 1 to 31744.

Default

By default, this value is 125 seconds

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for VLAN interface configuration. The query interval is the interval between General Queries sent by the Querier. By varying the query interval, an administrator may tune the number of IGMP messages on the network; larger values cause IGMP Queries to be sent less often.

Example

This example shows how to configure the IGMP snooping query interval to 300 seconds on VLAN 1000.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1000
GA-MLxxTPoE+(config-vlan)# ip igmp snooping query-interval 300
GA-MLxxTPoE+(config-vlan)#
```

8.1.11 ip igmp snooping query-max-response-time

This command is used to configure the maximum response time advertised in IGMP snooping queries. Use the **no** form of this command to revert to the default setting.

Syntax

- **ip igmp snooping query-max-response-time** *SECONDS*
- **no ip igmp snooping query-max-response-time**

Parameters

Parameters	Description
SECONDS	Specifies to set the maximum response time, in seconds, advertised in IGMP snooping queries. The range is from 1 to 25.

Default

By default, this value is 10 seconds.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for VLAN interface configuration. This command configures the period of which the group member can respond to an IGMP query message before the IGMP Snooping deletes the membership.

Example

This example shows how to configure the maximum response time to 20 seconds on an interface.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1000
GA-MLxxTPoE+(config-vlan)# ip igmp snooping query-max-response-time 20
GA-MLxxTPoE+(config-vlan)#
```

8.1.12 ip igmp snooping query-version

This command is used to configure the general query packet version sent by the IGMP snooping querier. Use the **no** form of this command to revert to the default setting.

Syntax

- **ip igmp snooping query-version** *NUMBER*
- **no ip igmp snooping query-version**

Parameters

Parameters	Description
NUMBER	Specifies the version of the IGMP general query sent by the IGMP snooping querier. The value is from 1 to 3.

Default

By default, this value is 3.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for VLAN interface configuration. The query version number setting will affect the querier electing. When configured to version 1, IGMP snooping will always act as the querier, and will not initiate new querier electing no matter what IGMP query packet is received. When configured to version 2 or version 3, IGMP snooping will initiate a new querier electing if any IGMPv2 or IGMPv3 query packet is received. When receiving an IGMPv1 query packet, IGMP snooping won't initiate a new querier electing.

Example

This example shows how to configure the query version to be 2 on VLAN 1000.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1000
GA-MLxxTPoE+(config-vlan)# ip igmp snooping query-version 2
GA-MLxxTPoE+(config-vlan)#
```

8.1.13 ip igmp snooping rate-limit

This command is used to configure the upper limit per second for ingress IGMP control packets. Use the **no** form of this command to disable the rate limit.

Syntax

- **ip igmp snooping rate-limit** *NUMBER*
- **no ip igmp snooping rate-limit**

Parameters

Parameters	Description
NUMBER	Specifies to configure the rate of the IGMP control packet that the Switch can process on a specific interface. The rate is specified in packets per second.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command is available for VLAN interface configuration, physical port or port-channel interface. The command configures the rate of IGMP control packet that can be processed by IGMP snooping.

Example

This example shows how to limit 30 packets per second on interface VLAN 1000.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1000
GA-MLxxTPoE+(config-vlan)# ip igmp snooping rate-limit 30
GA-MLxxTPoE+(config-vlan)#
```

8.1.14 ip igmp snooping robustness-variable

This command is used to set the robustness variable used in IGMP snooping. Use the **no** form of this command to revert to the default setting.

Syntax

- **ip igmp snooping robustness-variable** *VALUE*
- **no ip igmp snooping robustness-variable**

Parameters

Parameters	Description
VALUE	Specifies the robustness variable. The value is from 1 to 7.

Default

By default, this value is 2.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for VLAN interface configuration. The robustness variable provides fine-tuning to allow for expected packet loss on an interface. The value of the robustness variable is used in calculating the following IGMP message intervals:

- Group member interval – The amount of time that must pass before a multicast router decides there are no more members of a group on a network.
  This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval).
- Other querier present interval – The amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier.
  This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval).
- Last member query count – The number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable.

Users can increase this value if a subnet is expected to be loose.

Example

This example shows how to configure the robustness variable to be 3 on interface VLAN 1000.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1000
GA-MLxxTPoE+(config-vlan)# ip igmp snooping robustness-variable 3
GA-MLxxTPoE+(config-vlan)#
```

8.1.15 ip igmp snooping static-group

This command is used to configure an IGMP snooping static group. Use the **no** form of this command is used to delete a static group.

Syntax

- **ip igmp snooping static-group** *GROUP-ADDRESS* **interface** *INTERFACE-ID* [**,** | **-**]
- **no ip igmp snooping static-group** *GROUP-ADDRESS* [**interface** *INTERFACE-ID* [**,** | **-**]]

Parameters

Parameters	Description
GROUP-ADDRESS	Specifies an IP multicast group address.
interface *INTERFACE-ID*	Specifies an interface or an interface list. The interface can be a physical interface or a port-channel.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

By default, no static-group is configured.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for VLAN interface configuration. This command applies to IGMP snooping on a VLAN interface to statically add group membership entries and/or source records.
The **ip igmp snooping static-group** command allows the user to create an IGMP snooping static group in case that the attached host does not support the IGMP protocol.

Example

This example shows how to statically add a group and source records for IGMP snooping.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1
GA-MLxxTPoE+(config-vlan)# ip igmp snooping static-group 226.1.2.3 interface gi1/0/5
GA-MLxxTPoE+(config-vlan)#
```

8.1.16 show ip igmp snooping

This command is used to display IGMP snooping information on the Switch.

Syntax

- **show ip igmp snooping** [**vlan** *VLAN-ID*]

Parameters

Parameters	Description
vlan *VLAN-ID*	(Optional) Specifies the VLAN to be displayed.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display IGMP snooping information for all VLANs where IGMP snooping is enabled.

Example

This example shows how to display IGMP snooping configurations.

```
GA-MLxxTPoE+#show ip igmp snooping

IGMP snooping global state: Enabled

VLAN #1 configuration
    IGMP snooping state              : Enabled
    Fast leave                       : Disabled (host-based)
    Querier state                    : Disabled
    Query version                    : v3
    Query interval                   : 125 seconds
    Max response time                : 10 seconds
    Robustness value                 : 2
    Last member query interval       : 1 seconds
    Proxy reporting                  : Disabled (Source 0.0.0.0)
    Rate limit                       : 0

Total Entries: 1

GA-MLxxTPoE+#
```

8.1.17 show ip igmp snooping groups

This command is used to display IGMP snooping group information learned on the Switch.

Syntax

- **show ip igmp snooping groups [vlan** *VLAN-ID* **[, | -] | [***IP-ADDRESS***] [detail]**

Parameters

Parameters	Description
vlan *VLAN-ID*	(Optional) Specifies the VLAN interface to be displayed. If no VLAN is specified, IGMP snooping group information of all VLANs will be displayed, at which IGMP Snooping is enabled.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.

Parameters	Description
IP-ADDRESS	(Optional) Specifies the group IP address to be displayed. If no IP address is specified, all IGMP group information will be displayed.
detail	(Optional) Specifies to display the IGMP group detail information.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display IGMP snooping group information.

Example

This example shows how to display IGMP snooping group information.

```
GA-MLxxTPoE+# show ip igmp snooping groups

Total Group Entries : 1
Total Source Entries: 2

vlan1, 230.1.1.1
Learned on port: 1/0/3,1/0/5

GA-MLxxTPoE+#
```

8.1.18 show ip igmp snooping filter

This command is used to display IGMP snooping filter configuration information for all interfaces on the Switch or for a specified interface.

Syntax

- **show ip igmp snooping filter [interface** *INTERFACE-ID* **[, | -]]**

Parameters

Parameters	Description
interface *INTERFACE-ID*	(Optional) Specifies that the interface can be a physical interface or a port-channel. If no interface is specified, IGMP snooping filter information on all interface will be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display the IGMP snooping limit and access group information.

Example

This example shows how to display IGMP snooping filter information when no interface is specified.

```
GA-MLxxTPoE+#show ip igmp snooping filter


Gi1/0/1
    Rate limit: Not Configured
    Access group: Not Configured
    Groups/Channel Limit: Not Configured
Gi1/0/2
    Rate limit: 10pps
    Access group: Not Configured
    Groups/Channel Limit: Not Configured

GA-MLxxTPoE+#
```

This example shows how to display filter information of GigabitEthernet1/0/2.

```
GA-MLxxTPoE+#show ip igmp snooping filter interface gi1/0/2


Gi1/0/2
    Rate limit: 10pps
    Access group: Not Configured
    Groups/Channel Limit: Not Configured

GA-MLxxTPoE+#
```

8.1.19 show ip igmp snooping mrouter

This command is used to display IGMP snooping multicast router information that has been automatically learned and manually configured on the Switch.

Syntax

- **show ip igmp snooping mrouter [vlan** *VLAN-ID* **[, | -]]**

Parameters

Parameters	Description
vlan *VLAN-ID*	(Optional) Specifies the VLAN. If no VLAN is specified, IGMP snooping information on all VLANs will be displayed of which IGMP snooping is enabled.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display dynamically learned or manually configured multicast router interfaces.

Example

This example shows how to display IGMP snooping m-router information.

```
GA-MLxxTPoE+#show ip igmp snooping mrouter

VLAN    Ports
-----   ----------------------------
1       1/0/1-1/0/4 (static)

Total Entries: 1

GA-MLxxTPoE+#
```

8.1.20 show ip igmp snooping statistics

This command is used to display IGMP snooping statistics information on the Switch.

Syntax

- **show ip igmp snooping statistics** {**interface** [*INTERFACE-ID* [**,** | **-**]] | **vlan** [*VLAN-ID* [**,** | **-**]]}

Parameters

Parameters	Description
interface	Specifies to display statistics counters by interface.
INTERFACE-ID	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
vlan	Specifies to display statistics counters by VLAN.
VLAN-ID	(Optional) Specifies the VLAN ID to be displayed.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command displays the IGMP snooping related statistics information.

Example

This example shows how to display IGMP snooping statistics information.

```
GA-MLxxTPoE+#show ip igmp snooping statistics vlan 1


VLAN 1 Statistics:
  IGMPv1 Rx: Report 0, Query 0
  IGMPv2 Rx: Report 0, Query 0, Leave 0
  IGMPv3 Rx: Report 3, Query 0
  IGMPv1 Tx: Report 0, Query 0
  IGMPv2 Tx: Report 0, Query 0, Leave 0
  IGMPv3 Tx: Report 1, Query 2

Total Entries: 1

GA-MLxxTPoE+#
```

8.1.21 show ip igmp snooping static-group

This command is used to display statically configured IGMP snooping groups on the Switch.

Syntax

- **show ip igmp snooping static-group** [*GROUP-ADDRESS* | **vlan** *VLAN-ID*]

Parameters

Parameters	Description
GROUP-ADDRESS	(Optional) Specifies the group IP address to be displayed.
vlan *VLAN-ID*	(Optional) Specifies the VLAN ID to be displayed.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display statically configured IGMP snooping groups on the Switch. If no optional parameter is specified, all the information are displayed.

Example

This example shows how to display statically configured IGMP snooping groups.

```
GA-MLxxTPoE+#show ip igmp snooping static-group

VLAN ID  Group address    Interface
-------  ---------------  ------------------------
1        230.1.1.1        1/0/1-1/0/2

Total Entries: 1

GA-MLxxTPoE+#
```

8.1.22 ip igmp snooping unknown-data limit

Use this command to configure the maximum number of group entries, which are learned from the unknown multicast data by IGMP snooping. To delete (or remove) the configuration, use **no form** of this command.

Syntax

- **ip igmp snooping unknown-data limit** *NUMBER*
- **no ip igmp snooping unknown-data limit**

Parameters

Parameter	Description
NUMBER	Specifies the maximum number of group entries, which learn from unknown multicast data. The range is from 1 to 1024.

Default

128

8.2 MLD (Multicast Listener Discovery) Snooping Commands

8.2.1 clear ipv6 mld snooping statistics

This command is used to clear MLD snooping statistic counters on the Switch.

Syntax

- **clear ipv6 mld snooping statistics** {**all** | **vlan** *VLAN-ID* | **interface** *INTERFACE-ID*}

Parameters

Parameters	Description
all	Specifies to clear IPv6 MLD snooping statistics for all VLANs and all ports.
vlan *VLAN-ID*	Specifies the VLAN used. If no VLAN is specified, statistics for all VLANs are cleared.
interface *INTERFACE-ID*	Specifies the interface used.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to clear MLD snooping statistic counters on the Switch.

Example

This example shows how to clear all MLD snooping statistics.

```
GA-MLxxTPoE+# clear ipv6 mld snooping statistics all
GA-MLxxTPoE+#
```

8.2.2 ipv6 mld snooping

This command is used to enable MLD snooping. Use the **no** form of this command to disable MLD snooping.

Syntax

- **ipv6 mld snooping**
- **no ipv6 mld snooping**

Parameters

None

Default

MLD snooping is disabled on all VLAN interfaces.
The MLD snooping global state is disabled by default.

Command Mode

Interface Configuration Mode
Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

For a VLAN to operate with MLD snooping, both the global state and its interface state must be enabled. the setting of IGMP snooping and MLD snooping settings are independent on a VLAN, so they can be enabled simultaneously on the same VLAN.

Example

This example shows how to enable MLD snooping operation on VLANs that are MLD snooping enabled.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ipv6 mld snooping
GA-MLxxTPoE+(config)#
```

This example shows how to enable MLD snooping on VLAN 1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1
GA-MLxxTPoE+(config-vlan)# ipv6 mld snooping
GA-MLxxTPoE+(config-vlan)#
```

8.2.3 ipv6 mld snooping access-group

This command is used to restrict the receivers on a subnet to only join the multicast groups that are permitted in a standard IPv6 access list. Use the **no** form of this command to disable this function.

Syntax

- **ipv6 mld snooping access-group** *IPV6-ACCESS-LIST-NAME* [**vlan** *VLAN-ID*]
- **no ipv6 mld snooping access-group** [**vlan** *VLAN-ID*]

Parameters

Parameters	Description
IPV6-ACCESS-LIST-NAME	Specifies a standard IPv6 access list. To permit users to join a group (*, G), specify "any" in source address field and G in destination address field of the access list entry.
vlan *VLAN-ID*	(Optional) Specifies a Layer 2 VLAN and applies the filter to packets that arrive on the VLAN.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to restrict the multicast traffic receiver to join to a specific group. The destination address in the access list represents the multicast group address that is used to permit the receiver to join the multicast group or to deny the receiver from joining the multicast group.
This command is available for physical port or port-channel interface configuration.

Example

This example shows how to restrict the serviced MLD snooping group for GigabitEthernet1/0/1 to group FF1E::14. In the following example, an IPv6 access list named "mld_filter" is created and only permits the packets destined for group address FF1E::14. Then, "mld_filter" access group is associtate with GigabitEthernet1/0/1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#ipv6 access-list mld_filter
GA-MLxxTPoE+(config-ipv6-acl)#permit any host FF1E::14
GA-MLxxTPoE+(config-ipv6-acl)#end
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#ipv6 mld snooping access-group mld_filter
GA-MLxxTPoE+(config-if)#
```

8.2.4 ipv6 mld snooping fast-leave

This command is used to configure MLD snooping fast-leave on the interface. Use the no form of this command to disable the fast-leave or option on the specified interface.

Syntax

- ipv6 mld snooping fast-leave
- no ipv6 mld snooping fast-leave

Parameters

None

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command is only available for VLAN interface configuration. The **ipv6 mld snooping fast-leave** command allows MLD membership to be removed from a port immediately after receiving the leave message without using the group-specific or group-and-source-specific query mechanism.

Example

This example shows how to enable MLD snooping fast-leave on VLAN 1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1
GA-MLxxTPoE+(config-vlan)# ipv6 mld snooping fast-leave
GA-MLxxTPoE+(config-vlan)#
```

8.2.5 ipv6 mld snooping last-listener-query-interval

This command is used to configure the interval at which the MLD snooping querier sends MLD group-specific or group-source-specific (channel) query messages. Use the **no** form of this command to revert to the default setting.

Syntax

- **ipv6 mld snooping last-listener-query-interval** *SECONDS*
- **no ipv6 mld snooping last-listener-query-interval**

Parameters

Parameters	Description
SECONDS	Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. The range of this value is 1 to 25.

Default

By default, this value is 1 second.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command is only available for VLAN interface configuration. On receiving a Done message, the MLD snooping querier will assume that there are no local members on the interface if there are no reports received after the response time. Users can lower this interval to reduce the amount of time it takes a switch to detect the loss of the last member of a group.

Example

This example shows how to configure the last-listener query interval time to be 3 seconds.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1000
GA-MLxxTPoE+(config-vlan)# ipv6 mld snooping last-listener-query-interval 3
GA-MLxxTPoE+(config-vlan)#
```

8.2.6 ipv6 mld snooping limit

This command is used to set the limit of MLD snooping multicast groups or channels which layer 2 interface can join. Use the **no** form of this command to remove the limitation.

Syntax

- **ipv6 mld snooping limit** *NUMBER* [**exceed-action** {**drop** | **replace**}] [**except** *IPv6-ACCESS-LIST-NAME*] [**vlan** *VLAN-ID*]
- **no ipv6 mld snooping limit** [**vlan** *VLAN-ID*]

Parameters

Parameters	Description
NUMBER	Specifies the maximum number of MLD snooping groups that the interface can join. This value must between 1 and 1024.

Parameters	Description
exceed-action	(Optional) Specifies the action for handling newly learned groups when the limitation is exceeded.
drop	(Optional) Specifies that the new group will be dropped.
replace	(Optional) Specifies that the new group will replace the oldest group.
except *IPv6-ACCESS-LIST-NAME*	(Optional) Specifies a standard IPv6 access list. The group (*,G) or channel (S,G) permitted in the access list will be excluded from the limit. To permit a channel (S,G), S is specified in the source address field and G is specified in the destination address field of the access list entry. To permit a group (*,G), "any" is specified in the source address field and G is specified in the destination address field of the access list entry.
vlan *VLAN-ID*	(Optional) Specifies a Layer 2 VLAN and applies the filter to packets that arrive on that VLAN.

Default

By default, there is no limit.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command is available for physical port or port-channel interface configuration.

Example

This example shows how to set the limit of MLD snooping groups that GigabitEthernet1/0/4 with VLAN ID 1000 can join and specify the "mld_filter" access list to be excluded from the limit.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/4
GA-MLxxTPoE+(config-if)# ipv6 mld snooping limit 80 except mld_filter vlan 1000
GA-MLxxTPoE+(config-if)#
```

This example shows how to remove the limit of MLD snooping groups that port-channel 4 with VLAN ID 1000 can join.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface port-channel 4
GA-MLxxTPoE+(config-if)# no ipv6 mld snooping limit vlan 1000
GA-MLxxTPoE+(config-if)#
```

8.2.7 ipv6 mld snooping mrouter

This command is used to configure the specified interface(s) as router ports or ports forbidden from becoming IPv6 multicast router ports on the VLAN interface on the Switch. Use the **no** form of this command to remove the interface(s) from router ports or forbidden IPv6 multicast router ports.

Syntax

- **ipv6 mld snooping mrouter {interface** *INTERFACE-ID* **[, | -] | forbidden interface** *INTERFACE-ID* **[, | -]}**
- **no ipv6 mld snooping mrouter {interface** *INTERFACE-ID* **[, | -] | forbidden interface** *INTERFACE-ID* **[, | -]}**

Parameters

Parameters	Description
interface	Specifies a range of interfaces as being connected to multicast-enabled routers.
forbidden interface	Specifies a range of interfaces as not being connected to multicast-enabled routers.
INTERFACE-ID	Specifies an interface or an interface list. No space is allowed before and after the comma. The interface can be a physical interface or a port-channel.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

No IPv6 MLD snooping multicast router port is configured.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command is only available for VLAN interface configuration. To specify a multicast router port, the valid interface can be a physical port or a port-channel. The specified multicast router port must be the member port of the configured VLAN. The member port of a port channel cannot be specified.
The multicast router port can be either dynamically learned or statically configured into an MLD snooping entity. With the dynamic learning, the MLD snooping entity will listen to MLD and PIMv6 packets to identify whether the partner device is a router.

Example

This example shows how to configure GigabitEthernet1/0/1 as an MLD snooping multicast router port and GigabitEthernet1/0/2 as an MLD snooping forbidden multicast router port on VLAN 1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1
GA-MLxxTPoE+(config-vlan)# ipv6 mld snooping mrouter interface gi1/0/1
GA-MLxxTPoE+(config-vlan)# ipv6 mld snooping mrouter forbidden interface gi1/0/2
GA-MLxxTPoE+(config-vlan)#
```

8.2.8 ipv6 mld snooping proxy-reporting

This command is used to enable the proxy-reporting function. Use the **no** form of this command to disable the proxy-reporting function.

Syntax

- **ipv6 mld snooping proxy-reporting** [**source** *IPV6-ADDRESS*]
- **no ipv6 mld snooping proxy-reporting**

Parameters

Parameters	Description
source *IPV6-ADDRESS*	(Optional) Specifies the source IP address of proxy reporting.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command is only available for VLAN interface configuration. The proxy reporting function only works for MLDv1 traffic.
When the proxy reporting function is enabled, the received multiple MLD report or leave packets are integrated into one report before being sent to the router port. The proxy reporting source IP will be used as source IP of the report, and the zero IP address will be used when the proxy reporting source IP is not set. Interface MAC will be used as source MAC of the report. If the VLAN has no IP address configured, then system MAC will be used.

Example

This example shows how to enable MLD snooping proxy-reporting on VLAN 1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1
GA-MLxxTPoE+(config-vlan)# ipv6 mld snooping proxy-reporting
GA-MLxxTPoE+(config-vlan)#
```

8.2.9 ipv6 mld snooping querier

This command is used to enable the MLD snooping querier on the Switch. Use the **no** form of this command to disable the MLD snooping querier function.

Syntax

- **ipv6 mld snooping querier**
- **no ipv6 mld snooping querier**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command is only available for VLAN interface configuration. The interface must have an IPv6 address assigned to start the querier. The system will return a warning message if the VLAN has no IPv6 address. If the querier is enabled, but the IPv6 address is removed, the querier will be stopped.
If the system can play the querier role, the entity will listen for MLD query packets sent by other devices. If an MLD query message is received, the device with lower IPv6 address becomes the querier. If the MLD protocol is also enabled on the interface, the MLD snooping querier state will be disabled automatically.

Example

This example shows how to enable the MLD snooping querier state on VLAN 1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1
GA-MLxxTPoE+(config-vlan)# ipv6 mld snooping querier
GA-MLxxTPoE+(config-vlan)#
```

8.2.10 ipv6 mld snooping query-interval

This command is used to configure the interval at which the MLD snooping querier sends MLD general query messages. Use the **no** form of this command to revert to the default setting.

Syntax

- **ipv6 mld snooping query-interval** *SECONDS*
- **no ipv6 mld snooping query-interval**

Parameters

Parameters	Description
SECONDS	Specifies the interval at which the designated router sends MLD general query messages. The range is from 1 to 31744.

Default

By default, this value is 125 seconds.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command is only available for VLAN interface configuration. The query interval is the interval between general queries sent by the querier. By varying the query interval, an administrator may tune the number of MLD messages on the network. Larger values cause MLD Queries to be sent less often.

Example

This example shows how to configure the MLD snooping query interval to 300 seconds on VLAN 1000.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1000
GA-MLxxTPoE+(config-vlan)# ipv6 mld snooping query-interval 300
GA-MLxxTPoE+(config-vlan)#
```

8.2.11 ipv6 mld snooping query-max-response-time

This command is used to configure the maximum response time advertised in MLD snooping queries. Use the **no** form of this command to revert to the default setting.

Syntax

- **ipv6 mld snooping query-max-response-time** *SECONDS*
- **no ipv6 mld snooping query-max-response-time**

Parameters

Parameters	Description
SECONDS	Specifies to set the maximum response time, in seconds, advertised in MLD snooping queries. The range is from 1 to 25.

Default

By default, this value is 10 seconds.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command is only available for VLAN interface configuration. This command configures the period of which the group member can respond to an MLD query message before MLD snooping deletes the membership.

Example

This example shows how to configure the maximum response time to 20 seconds on an interface.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1000
GA-MLxxTPoE+(config-vlan)# ipv6 mld snooping query-max-response-time 20
GA-MLxxTPoE+(config-vlan)#
```

8.2.12 ipv6 mld snooping query-version

This command is used to configure the general query packet version sent by the MLD snooping querier. Use the **no** form of this command to revert to the default setting.

Syntax

- **ipv6 mld snooping query-version {1 | 2}**
- **no ipv6 mld snooping query-version**

Parameters

Parameters	Description
1	Specifies that the version of the MLD general query sent by MLD snooping querier is 1.
2	Specifies that the version of the MLD general query sent by MLD snooping querier is 2.

Default

By default, the version number is 2.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command is only available for VLAN interface configuration.

Example

This example shows how to configure the query version to be 1 on VLAN 1000.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1000
GA-MLxxTPoE+(config-vlan)# ipv6 mld snooping query-version 1
GA-MLxxTPoE+(config-vlan)#
```

8.2.13 ipv6 mld snooping rate-limit

This command is used to configure the upper limit of ingress MLD control packets per second. Use the **no** form of this command to disable the rate limit.

Syntax

- **ipv6 mld snooping rate-limit** *NUMBER*
- **no ipv6 mld snooping rate-limit**

Parameters

Parameters	Description
NUMBER	Specifies to configure the rate of the MLD control packet that the Switch can process on a specific interface. The rate is specified in packets per second.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command is available for VLAN interface configuration, physical port or port-channel interface. The command configures the rate of MLD control packets that are allowed per interface.

Example

This example shows how to limit 30 packets per second on interface VLAN 1000.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1000
GA-MLxxTPoE+(config-vlan)# ipv6 mld snooping rate-limit 30
GA-MLxxTPoE+(config-vlan)#
```

8.2.14 ipv6 mld snooping robustness-variable

This command is used to set the robustness variable used in MLD snooping. Use the **no** form of this command to revert to the default setting.

Syntax

- **ipv6 mld snooping robustness-variable** *VALUE*
- **no ipv6 mld snooping robustness-variable**

Parameters

Parameters	Description
VALUE	Specifies the robustness variable. The value is from 1 to 7.

Default

By default, this value is 2.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command is only available for VLAN interface configuration.
The robustness variable provides fine-tuning to allow for expected packet loss on an interface. The value of the robustness variable is used in calculating the following MLD message intervals:

- Group member interval – The amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval).
- Other querier present interval – The amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval).
- Last member query count – The number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable.

This value can be increased if a subnet is expected to lose packets.

Example

This example shows how to configure the robustness variable to be 3 on interface VLAN 1000.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1000
GA-MLxxTPoE+(config-vlan)# ipv6 mld snooping robustness-variable 3
GA-MLxxTPoE+(config-vlan)#
```

8.2.15 ipv6 mld snooping static-group

This command is used to configure an MLD snooping static group. Use the **no** form of this command to delete a static group.

Syntax

- **ipv6 mld snooping static-group** *IPV6-ADDRESS* **interface** *INTERFACE-ID* **[, | -]**
- **no ipv6 mld snooping static-group** *IPV6-ADDRESS* **[interface** *INTERFACE-ID* **[, | -]]**

Parameters

Parameters	Description
IPV6-ADDRESS	Specifies an IPv6 multicast group address.
interface *INTERFACE-ID*	Specifies the interfaces to be used.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

No static-group is configured.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command is only available for VLAN interface configuration. This command applies to MLD snooping on a VLAN interface to statically add group membership entries and/or source records.
The **ipv6 mld snooping static-group** command allows the user to create an MLD snooping static group in case that the attached host does not support the MLD protocol.

Example

This example shows how to statically add group and/or source records for MLD snooping.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# vlan 1
GA-MLxxTPoE+(config-vlan)# ipv6 mld snooping static-group FF02::12:03 interface gi1/0/5
GA-MLxxTPoE+(config-vlan)#
```

8.2.16 show ipv6 mld snooping

This command is used to display MLD snooping information on the Switch.

Syntax

- **show ipv6 mld snooping [vlan** *VLAN-ID*]

Parameters

Parameters	Description
vlan *VLAN-ID*	(Optional) Specifies the VLAN to be displayed.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

If no optional parameter is specified, MLD snooping information for all VLANs with MLD snooping enabled will be displayed.

Example

This example shows how to display MLD snooping configuration.

```
GA-MLxxTPoE+# show ipv6 mld snooping

MLD snooping global state: Enabled

VLAN #1 configuration
    MLD snooping state           : Enabled
    Fast leave                   : Disabled (host-based)
    Proxy reporting              : Disabled (Source ::)
    Querier state                : Disabled
    Query version                : v2
    Query interval               : 125 seconds
    Max response time            : 10 seconds
    Robustness value             : 2
    Last listener query interval : 1 seconds
    Rate limit                   : 50

Total Entries: 1

GA-MLxxTPoE+#
```

8.2.17 show ipv6 mld snooping filter

This command is used to display MLD snooping filter information for specified interface(s).

Syntax

- **show ipv6 mld snooping filter [interface** *INTERFACE-ID* **[, | -]]**

Parameters

Parameters	Description
interface *INTERFACE-ID*	(Optional) Specifies the interfaces to be displayed. The interface can be a physical interface or a port-channel.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display MLD snooping limit and access group information. If no optional parameter is specified, MLD snooping filter information for all interfaces will be displayed.

Example

This example shows how to display filter information when no interface is specified.

```
GA-MLxxTPoE+#show ipv6 mld snooping filter


Gi1/0/1
    Rate limit: Not Configured
    Access group: mld_filter
    Groups/Channel Limit: Not Configured

GA-MLxxTPoE+#
```

8.2.18 show ipv6 mld snooping groups

This command is used to display MLD snooping group information learned on the Switch.

Syntax

- **show ipv6 mld snooping groups** [*IPV6-ADDRESS* | **vlan** *VLAN-ID*] [**detail**]

Parameters

Parameters	Description
IPV6-ADDRESS	(Optional) Specifies the group IP address. If no IPv6 address is specified, all MLD group information will be displayed.
vlan *VLAN-ID*	(Optional) Specifies the VLAN ID to be displayed. If no VLAN is specified, MLD group information about all VLANs will be displayed.

Parameters	Description
,	(Optional) Specifies a series of VLANs, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.
detail	(Optional) Specifies to display the MLD group detail information.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display MLD group information by command.

Example

This example shows how to display MLD snooping group information.

```
GA-MLxxTPoE+# show ipv6 mld snooping groups

Total Group Entries : 1
Total Source Entries: 1

vlan1, FF1E::1
Learned on port: 1/0/3

GA-MLxxTPoE+#
```

8.2.19 show ipv6 mld snooping mrouter

This command is used to display MLD snooping multicast router information that has been automatically learned and manually configured on the Switch.

Syntax

- **show ipv6 mld snooping mrouter [vlan** *VLAN-ID* **[, | -]]**

Parameters

Parameters	Description
vlan *VLAN-ID*	(Optional) Specifies the VLAN ID to be displayed. If no VLAN is specified, MLD snooping Multicast Router Information on all VLANs will be displayed.
,	(Optional) Specifies a series of VLANs, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display dynamically learned or manually configured multicast router interfaces.

Example

This example shows how to display MLD snooping multicast router information.

```
GA-MLxxTPoE+#show ipv6 mld snooping mrouter

VLAN    Ports
-----   ----------------------------
1       Gi1/0/1 (static)
        Gi1/0/2 (forbidden)

Total Entries: 1

GA-MLxxTPoE+#
```

8.2.20 show ipv6 mld snooping static-group

This command is used to display statically configured MLD snooping groups on the Switch.

Syntax

- **show ipv6 mld snooping static-group** [*GROUP-ADDRESS* | **vlan** *VLAN-ID*]

Parameters

Parameters	Description
GROUP-ADDRESS	(Optional) Specifies the group IPv6 address to be displayed.
vlan *VLAN-ID*	(Optional) Specifies the VLAN ID to be displayed.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command is used to display statically configured MLD snooping groups on the Switch. If no optional parameter is specified, all information will be displayed.

Example

This example shows how to display statically configured MLD snooping groups.

```
GA-MLxxTPoE+#show ipv6 mld snooping static-group

VLAN ID Group address                          Interface
------- ------------------------------------- ------------------
1       FF02::12:3                            Gi1/0/5

Total Entries: 1

GA-MLxxTPoE+#
```

8.2.21 show ipv6 mld snooping statistics

This command is used to display MLD snooping statistics information on the Switch.

Syntax

- **show ipv6 mld snooping statistics {interface [***INTERFACE-ID***[, | -]] | vlan [***VLAN-ID***[, | -]]}**

Parameters

Parameters	Description
interface	Specifies to display statistics counters by interface.
INTERFACE-ID	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
vlan	Specifies to display statistics counters by VLAN.
VLAN-ID	(Optional) Specifies the VLAN ID to be displayed.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command displays the MLD snooping related statistics information.

Example

This example shows how to display MLD snooping statistics information.

```
GA-MLxxTPoE+#show ipv6 mld snooping statistics interface

Interface Gi1/0/1
  Rx: v1Report 0, v2Report 14, Query 0, v1Done 0
  Tx: v1Report 0, v2Report 0, Query 0, v1Done 0

Interface Gi1/0/2
  Rx: v1Report 0, v2Report 0, Query 0, v1Done 0
  Tx: v1Report 0, v2Report 0, Query 0, v1Done 0

Interface Gi1/0/3
  Rx: v1Report 0, v2Report 0, Query 0, v1Done 0
  Tx: v1Report 0, v2Report 0, Query 0, v1Done 0

Interface Gi1/0/4
  Rx: v1Report 0, v2Report 0, Query 0, v1Done 0
  Tx: v1Report 0, v2Report 0, Query 0, v1Done 0

Interface Gi1/0/5
  Rx: v1Report 0, v2Report 0, Query 0, v1Done 0
  Tx: v1Report 0, v2Report 0, Query 0, v1Done 0

Interface Gi1/0/6
  Rx: v1Report 0, v2Report 0, Query 0, v1Done 0
  Tx: v1Report 0, v2Report 0, Query 0, v1Done 0
--More--
```

9 Network Management

9.1 SNMP (Simple Network Management Protocol) Commands

9.1.1 show snmp

This command is used to display the SNMP settings.

Syntax

- show snmp {community | host | view | group | engineID}

Parameters

Parameters	Description
community	Specifies to display SNMP community information.
host	Specifies to display SNMP trap recipient information.
view	Specifies to display SNMP view information.
group	Specifies to display SNMP group information.
engineID	Specifies to display SNMP local engine ID information.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

This command displays the SNMP information. When displaying SNMP community strings, the SNMPv1 or SNMPv2c user created will not be displayed.

Example

This example shows how to display SNMP community information.

```
GA-MLxxTPoE+#show snmp community

Community : public
 Access : read-only
 View : CommunityView

Community : private
 Access : read-write
 View : CommunityView

GA-MLxxTPoE+#
```

This example shows how to display the SNMP server host setting.

```
GA-MLxxTPoE+#show snmp host

Host IP Address  : 10.90.90.1
SNMP Version     : V1
Community Name   : public
UDP Port         : 162

Total Entries: 1

GA-MLxxTPoE+#
```

This example shows how to display the MIB view setting.

```
GA-MLxxTPoE+#show snmp view

restricted(included) 1.3.6.1.2.1.1
restricted(included) 1.3.6.1.2.1.11
restricted(included) 1.3.6.1.6.3.10.2.1
restricted(included) 1.3.6.1.6.3.11.2.1
restricted(included) 1.3.6.1.6.3.15.1.1
CommunityView(included) 1
CommunityView(excluded) 1.3.6.1.6.3
CommunityView(included) 1.3.6.1.6.3.1

Total Entries: 8

GA-MLxxTPoE+#
```

This example shows how to display the SNMP group setting.

```
GA-MLxxTPoE+#show snmp group

GroupName: public                                SecurityModel: v1
  ReadView      : CommunityView                  WriteView     :
  NotifyView    : CommunityView
  IP access control list:

GroupName: public                                SecurityModel: v2c
  ReadView      : CommunityView                  WriteView     :
  NotifyView    : CommunityView
  IP access control list:

GroupName: initial                               SecurityModel: v3/noauth
  ReadView      : restricted                     WriteView     :
  NotifyView    : restricted
  IP access control list:

GroupName: private                               SecurityModel: v1
  ReadView      : CommunityView                  WriteView     : CommunityView
  NotifyView    : CommunityView
  IP access control list:

GroupName: private                               SecurityModel: v2c
  ReadView      : CommunityView                  WriteView     : CommunityView
  NotifyView    : CommunityView
--More--
```

This example shows how to display the SNMP engine ID.

```
GA-MLxxTPoE+#show snmp engineID

Local SNMP engineID: 800000ab03f07d6834001000

GA-MLxxTPoE+#
```

9.1.2 show snmp user

This command is used to display information about the configured SNMP user.

Syntax

- **show snmp user** [*USER-NAME*]

Parameters

Parameters	Description
USER-NAME	(Optional) Specifies the name of a specific user to display SNMP information.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

When the username argument is not specified, all configured users will be displayed. The community string created will not displayed by this command.

Example

This example shows how to display SNMP users.

```
GA-MLxxTPoE+#show snmp user

User Name: initial
  Security Model: 3
  Group Name: initial
  Authentication Protocol: None
  Privacy Protocol: None
  Engine ID: 800000ab03f07d6834001000
  IP access control list:

Total Entries: 1

GA-MLxxTPoE+#
```

9.1.3 snmp-server community

This command is used to configure the community string to access the SNMP. Use the **no** form of this command to remove the community string.

Syntax

- **snmp-server community** [0 | 7] *COMMUNITY-STRING* [**view** *VIEW-NAME*] [**ro** | **rw**] [**access** *IP-ACL-NAME*] [**context** *CONTEXT*]
- **no snmp-server community** [0 | 7] *COMMUNITY-STRING*

Parameters

Parameters	Description
0 *COMMUNITY-STRING*	(Optional) Specifies the community string in the plain text form with a maximum of 32 alphanumeric characters. This is the default option.
7 *COMMUNITY-STRING*	(Optional) Specifies the community string in the encrypted form.
view *VIEW-NAME*	(Optional) Specifies a view name of a previously defined view. It defines the view accessible by the SNMP community.
ro	(Optional) Specifies read-only access.
rw	(Optional) Specifies read-write access.
access *IP-ACL-NAME*	(Optional) Specifies the name of the standard access list to control the user to use this community string to access to the SNMP agent. Specifies the valid user in the source address field of the access list entry.
context *CONTEXT*	(Optional) Specifies the SNMP context name.

Default

Community	View Name	Access right
private	CommunityView	Read/Write
public	CommunityView	Read Only

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

This command provides an easy way to create a community string for SNMPv1 and SNMPv2c management. When creating a community with the **snmp-server community** command, two SNMP group entries, one for SNMPv1 and one for SNMPv2c, which has the community name as their group names are created. If the view is not specified, it is permitted to access all objects.

Example

This example shows how a MIB view “interfacesMibView” is created and a community string “comaccess” which can do read write access the interfacesMibView view is created.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
GA-MLxxTPoE+(config)# snmp-server community comaccess view interfacesMibView rw
GA-MLxxTPoE+(config)#
```

9.1.4 snmp-server engineID local

This command is used to specify the SNMP engine ID on the local device. Use the **no** form of this command to revert to the default setting.

Syntax

- **snmp-server engineID local** *ENGINEID-STRING*
- **no snmp-server engineID local**

Parameters

Parameters	Description
ENGINEID-STRING	Specifies the engine ID string of a maximum of 24 characters.

Default

A default SNMP engine ID is automatically generated.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

An SNMP engine ID is not displayed or stored in the running configuration. The SNMP engine ID is a unique string to identify the device. A string is generated by default. If you configure a string less than 24 characters, it will be filled with trailing zeros up to 24 characters.

Example

This example shows how to configure the SNMP engine ID to 33220000000000000000000.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server engineID local 3322
GA-MLxxTPoE+(config)#
```

9.1.5 snmp-server group

This command is used to configure an SNMP group. Use the **no** form of this command to remove a SNMP group or remove a group from using a specific security model.

Syntax

- **snmp-server group** *GROUP-NAME* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *READ-VIEW*] [**write** *WRITE-VIEW*] [**notify** *NOTIFY-VIEW*] [**access** *IP-ACL-NAME*] [**context** *CONTEXT*]
- **no snmp-server group** *GROUP-NAME* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}}

Parameters

Parameters	Description
GROUP-NAME	Specifies the group name of a maximum of 32 characters. The syntax is general string that does not allow space.
v1	Specifies that the group user can use the SNMPv1 security model.
v2c	Specifies that the group user can use the SNMPv2c security model.
v3	Specifies that the group user can use the SNMPv3 security model.
auth	Specifies to authenticate the packet but not encrypt it.
noauth	Specifies not to authenticate and not to encrypt the packet.
priv	Specifies to authenticate and encrypt the packet.
read *READ-VIEW*	(Optional) Specifies a read-view that the group user can access.
write *WRITE-VIEW*	(Optional) Specifies a write-view that the group user can access.
notify *NOTIFY-VIEW*	(Optional) Specifies a notify-view that the group user can access. The notify view describes the object that can be reported its status via trap packets to the group user.

Parameters	Description
access *IP-ACL-NAME*	(Optional) Specifies the standard IP access control list (ACL) to associate with the group.
context *CONTEXT*	(Optional) Specifies the SNMP context name.

Default

Group Name	Version	Security Level	Read View Name	Write View Name	Notify View Name
Initial	SNMPv3	noauth	Restricted	None	Restricted
ReadGroup	SNMPv1	noauth	Community View	None	Community View
ReadGroup	SNMPv2c	noauth	Community View	None	Community View
WriteGroup	SNMPv1	noauth	Community View	Community View	Community View
WriteGroup	SNMPv2c	noauth	Community View	Community View	Community View

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

An SNMP group defines a user group by specifying the allowed security model, the read-view, the write-view, and the notification view. The security model defines that the group user is allowed to use the specified version of SNMP to access the SNMP agent,
The same group name can be created with security models SNMPv1, SNMPv2c, and SNMPv3 at the same time. For SNMPv3, it can be created for SNMPv3 auth and SNMPv3 priv at the same time.
To update the view profile for a group for a specific security mode, delete and create the group with the new view profile.
The read-view defines the MIB objects that the group user is allowed to read. If read-view is not specified, then Internet OID space 1.3.6.1 can be read.
The write-view defines the MIB objects that the group user is allowed to write. If write-view is not specified, then no MIB objects can be written.

The notification view defines the MIB objects that the system can report its status in the notification packets to the trap managers that are identified by the specified group user (act as community string). If notify-view is not specified, then no MIB objects can be reported.

Example

This example shows how to create the SNMP server group "guestgroup" for SNMPv3 access and SNMPv2c.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
GA-MLxxTPoE+(config)# snmp-server group guestgroup v3 auth read interfacesMibView
GA-MLxxTPoE+(config)# snmp-server group guestgroup v2c read CommunityView write
CommunityView
GA-MLxxTPoE+(config)#
```

9.1.6 snmp-server host

This command is used to specify the recipient of the SNMP notification. Use the **no** form of this command to remove the recipient.

Syntax

- **snmp-server host** {*IP-ADDRESS* | *IPV6-ADDRESS*} [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}] *COMMUNITY-STRING* [**port** *PORT-NUMBER*]
- **no snmp-server host** {*IP-ADDRESS* | *IPV6-ADDRESS*}

Parameters

Parameters	Description
IP-ADDRESS	Specifies the IPv4 address of the SNMP notification host.
IPV6-ADDRESS	Specifies the IPv6 address of the SNMP notification host.
version	(Optional) Specifies the version of the SNMP used to send the traps. If not specified, the default is SNMPv1 **1** - SNMPv1. **2c** - SNMPv2c. **3** - SNMPv3.
auth	(Optional) Specifies to authenticate the packet but not to encrypt it.
noauth	(Optional) Specifies not to authenticate and to encrypt the packet.
priv	(Optional) Specifies to both authenticate and to encrypt the packet.

Parameters	Description
COMMUNITY-STRING	Specifies the community string to be sent with the notification packet. If the version is 3, the community string is used as the username as defined in the **snmp-sever user** command.
port *PORT-NUMBER*	(Optional) Specifies the UDP port number. The default trap UDP port number is 162. The range of UDP port numbers is from 1 to 65535. Some port numbers may conflict with other protocols.

Default

By default, the version used is 1.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

SNMP notifications are sent as trap packets. The user should create at least one recipient of a SNMP notification by using the **snmp-server host** command in order for the Switch to send the SNMP notifications. Specify the version of the notification packet for the created user. For SNMPv1 and SNMPv2c, the notification will be sent in the trap protocol data unit (PDU). For SNMPv3, the notification will be sent in the SNMPv2-TRAP-PDU with the SNMPv3 header.
When specifying to send the trap packets in SNMPv1 or SNMPv2c to a specific host, the specified community string acts as the community string in the trap packets.
When specifying to send the trap packets in SNMPv3 to a specific host, whether to do authentication and encryption in the sending of the packet should be specified. The specified community string acts as the username in the SNMPv3 packet. The user must be created first using the **snmp-server user** command or **snmp-server user v3** command.
In the sending of the trap packet, the system will check the notification view associated with the specified user (or community name). If the binding variables to be sent with the trap packet are not in the notification view, the notification will not be sent to this host.

Example

This example shows how to configure the trap recipient 163.10.50.126 with version 1 with community string “comaccess”.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server community comaccess rw
GA-MLxxTPoE+(config)# snmp-server host 163.10.50.126 version 1 comaccess
GA-MLxxTPoE+(config)#
```

This example shows how to configure the trap recipient 163.10.50.126 with version 3 authentication security level and with the username “useraccess”.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server group groupaccess v3 auth read CommunityView write
CommunityView
GA-MLxxTPoE+(config)# snmp-server user useraccess groupaccess v3 auth md5 12345678
GA-MLxxTPoE+(config)# snmp-server host 163.10.50.126 version 3 auth useraccess
GA-MLxxTPoE+(config)#
```

This example shows how to configure the trap recipient 163.10.50.126 with version 1 with the community string “comaccess”. The UDP port number is configured to 50001.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server community comaccess rw
GA-MLxxTPoE+(config)# snmp-server host 163.10.50.126 version 1 comaccess port 50001
GA-MLxxTPoE+(config)#
```

9.1.7 snmp-server user

This command is used to create an SNMP user. Use the **no** form of this command to remove an SNMP user.

Syntax

- **snmp-server user** *USER-NAME GROUP-NAME* {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *AUTH-PASSWORD* [**priv** *PRIV-PASSWORD*]]} [**access** *IP-ACL-NAME*]
- **no snmp-server user** *USER-NAME GROUP-NAME* {**v1** | **v2c** | **v3**}

Parameters

Parameters	Description
USER-NAME	Specifies a username of a maximum of 32 characters. The syntax is general string that does not allow spaces.
GROUP-NAME	Specifies the name of the group to which the user belongs. The syntax is general string that does not allow spaces.
v1	Specifies that the user uses the SNMPv1 security mode.
v2c	Specifies that the user uses the SNMPv2c security mode.

Parameters	Description
v3	Specifies that the user uses the SNMPv3 security mode.
encrypted	(Optional) Specifies that the following password is in encrypted format.
auth	(Optional) Specifies the authentication level.
md5	(Optional) Specifies to use HMAC-MD5-96 authentication.
sha	(Optional) Specifies to use HMAC-SHA-96 authentication.
AUTH-PASSWORD	(Optional) Specifies the authentication password in the plain-text form. This password is 8 to 16 octets for MD5 and 8 to 20 octets for SHA. If the **encrypted** parameter is specified, the length is 32 for MD5 and 40 for SHA. The format is a hexadecimal value.
priv	(Optional) Specifies the type of encryption.
PRIV-PASSWORD	Specifies the private password in the plain-text form. This password can be up to 64 characters. If the **encrypted** parameter is specified, the length is fixed to 16 octets
access *IP-ACL-NAME*	(Optional) Specifies the standard IP ACL to associate with the user.

Default

By default, there is one user.
User Name: initial.
Group Name: initial.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

To create an SMNP user, specify the security model that the user uses and the group that the user is created for. To create an SNMPv3 user, the password used for authentication and encryption needs to be specified.
An SNMP user is unable to be deleted if it has been associated with a SNMP server host.

Example

This example shows how the plain-text password is configured for the user “user1” in the SNMPv3 group public.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server user user1 public v3 auth md5 authpassword priv
privpassword
GA-MLxxTPoE+(config)#
```

This example shows how the MD5 digest string is used instead of the plain text password.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server user user1 public v3 encrypted auth md5
00112233445566778899AABBCCDDEEFF
GA-MLxxTPoE+(config)#
```

9.1.8 snmp-server view

This command is used to create or modify a view entry. Use the **no** form of this command to remove a specified SNMP view entry.

Syntax

- **snmp-server view** *VIEW-NAME OID-TREE* **{included | excluded}**
- **no snmp-server view** *VIEW-NAME*

Parameters

Parameters	Description
VIEW-NAME	Specifies the name of the view entry. The valid length is 1 to 32 characters. The syntax is general string that does not allow spaces.
OID-TREE	Specifies the object identifier of the ASN.1 sub-tree to be included or excluded from the view. To identify the sub-tree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. Use the asterisk (*) wildcard in a single sub-identifier to specify a sub-tree family.
included	Specifies the sub-tree to be included in the SNMP view.
excluded	Specifies the sub-tree to be excluded from the SNMP view.

Default

VIEW-NAME	OID-TREE	View Type
Restricted	1.3.6.1.2.1.1	Included

VIEW-NAME	OID-TREE	View Type
Restricted	1.3.6.1.2.1.11	Included
Restricted	1.3.6.1.6.3.10.2.1	Included
Restricted	1.3.6.1.6.3.11.2.1	Included
Restricted	1.3.6.1.6.3.15.1.1	Included
CommunityView	1	Included
CommunityView	1.3.6.1.6.3	Excluded
CommunityView	1.3.6.1.6.3.1	Included

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to create a view of MIB objects.

Example

This example shows how to create a MIB view called “interfacesMibView” and define an SNMP group “guestgroup” with “interfacesMibView” as the read view.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
GA-MLxxTPoE+(config)# snmp-server group guestgroup v3 auth read interfacesMibView
GA-MLxxTPoE+(config)#
```

9.1.9 show snmp trap link-status

This command is used to display the per interface link status trap state.

Syntax

- **show snmp trap link-status [interface** *INTERFACE-ID* **[, | -]]**

Parameters

Parameters	Description
interface *INTERFACE-ID*	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display per interface link up/down trap state.

Example

This example shows how to display the interface's link up/down trap state for GigabitEthernet1/0/1 to 1/0/9.

```
GA-MLxxTPoE+#show snmp trap link-status interface gi1/0/1-9

Interface           Trap state
-------------       -------------
Gi1/0/1             Enabled
Gi1/0/2             Enabled
Gi1/0/3             Enabled
Gi1/0/4             Enabled
Gi1/0/5             Enabled
Gi1/0/6             Enabled
Gi1/0/7             Enabled
Gi1/0/8             Enabled
Gi1/0/9             Enabled


GA-MLxxTPoE+#
```

9.1.10 show snmp-server

This command is used to display the SNMP server's global state settings and trap related settings.

Syntax

- **show snmp-server [traps]**

Parameters

Parameters	Description
traps	(Optional) Specifies to display trap related settings.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use the **show snmp-server** command to display the SNMP server global state settings.
Use the **show snmp-server traps** command to display trap related settings.

Example

This example shows how to display the SNMP server configuration.

```
GA-MLxxTPoE+#show snmp-server

SNMP Server  : Enabled
Name         : Switch
Location     :
Contact      :
SNMP UDP Port    : 161
SNMP Response Broadcast Request    : Enabled

GA-MLxxTPoE+#
```

This example shows how to display trap related settings.

```
GA-MLxxTPoE+#show snmp-server traps

Global Trap State : Enabled
Individual Trap State:
    Authentication          : Enabled
    Linkup                  : Enabled
    Linkdown                : Enabled
    Coldstart               : Disabled
    Warmstart               : Disabled

GA-MLxxTPoE+#
```

9.1.11 show snmp-server trap-sending

This command is used to display the per port SNMP trap sending state.

Syntax

- **show snmp-server trap-sending [interface** *INTERFACE-ID* **[, | -]]**

Parameters

Parameters	Description
interface *INTERFACE-ID*	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display the per port trap sending state. If no optional parameter is specified, all ports will be displayed.

Example

This example shows how to display the trap sending state for gi1/0/1 to 1/0/9.

```
GA-MLxxTPoE+#show snmp-server trap-sending interface gi1/0/1-9

       Port                          Trap Sending
-----------------                   ---------------
 Gi1/0/1                              Enabled
 Gi1/0/2                              Enabled
 Gi1/0/3                              Enabled
 Gi1/0/4                              Enabled
 Gi1/0/5                              Enabled
 Gi1/0/6                              Enabled
 Gi1/0/7                              Enabled
 Gi1/0/8                              Enabled
 Gi1/0/9                              Enabled
GA-MLxxTPoE+#
```

9.1.12 snmp-server

This command is used to enable the SNMP agent. Use the **no** form of this command to disable the SNMP agent.

Syntax

- **snmp-server**
- **no snmp-server**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The SNMP manager manages a SNMP agent by sending SNMP requests to agents and receiving SNMP responses and notifications from agents. The SNMP server on the agent must be enabled before the agent can be managed.

Example

This example shows how to enable the SNMP server.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server
GA-MLxxTPoE+(config)#
```

9.1.13 snmp-server contact

This command is used to configure the system contact information for the device. Use the **no** form of this command to remove the setting.

Syntax

- **snmp-server contact** *TEXT*
- **no snmp-server contact**

Parameters

Parameters	Description
TEXT	Specifies a string for describing the system contact information. The maximum length is 255 characters The syntax is a general string that allows spaces.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command configures the system contact information for management of the device.

Example

This example shows how to configure the system contact information with the string MIS Department II.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server contact MIS Department II
GA-MLxxTPoE+(config)#
```

9.1.14 snmp-server enable traps

This command is used to enable the sending of trap packets globally. Use the **no** form of this command to disable the sending of trap packets.

Syntax

- **snmp-server enable traps**
- **no snmp-server enable traps**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command enables the device to send the SNMP notification traps globally. To configure the router to send these SNMP notifications, enter the **snmp-server enable traps** command to enable the global setting.

Example

This example shows how to enable the SNMP traps global sending state.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server enable traps
GA-MLxxTPoE+(config)#
```

9.1.15 snmp-server enable traps snmp

This command is used to enable the sending of all or specific SNMP notifications. Use the **no** form of this command to disable sending of all or specific SNMP notifications.

Syntax

- **snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [warmstart]**
- **no snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [warmstart]**

Parameters

Parameters	Description
authentication	(Optional) Specifies to control the sending of SNMP authentication failure notifications. An authenticationFailuretrap is generated when the device receives an SNMP message that is not properly authenticated. The authentication method depends on the version of SNMP being used. For SNMPv1 or SNMPv2c, authentication failure occurs if packets are formed with an incorrect community string. For SNMPv3, authentication failure occurs if packets are formed with an incorrect SHA/MD5 authentication key.
linkup	(Optional) Specifies to control the sending of SNMP linkUp notifications. A linkup (3) trap signifies is generated when the device recognizes that one of the communication links has come up.
linkdown	(Optional) Specifies to control the sending of SNMP linkDown notifications. A linkDown (2) trap is generated when the device recognizes a failure in one of the communication links.
coldstart	(Optional) Specifies to control the sending of SNMP coldStart notifications.
warmstart	(Optional) Specifies to control the sending of SNMP warmStart notifications.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command controls the sending of SNMP standard notification traps. To enable the sending of notification traps, the global setting must be enabled too.

Example

This example shows how to enable the router to send all SNMP traps to the host 10.9.18.100 using the community string defined as public.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server enable traps
GA-MLxxTPoE+(config)# snmp-server enable traps snmp
GA-MLxxTPoE+(config)# snmp-server host 10.9.18.100 version 2c public
GA-MLxxTPoE+(config)#
```

This example shows how to enable the SNMP authentication traps.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server enable traps snmp authentication
GA-MLxxTPoE+(config)#
```

9.1.16 snmp-server location

This command is used to configure the system's location information. Use the **no** form of this command to remove the setting.

Syntax

- **snmp-server location** *TEXT*
- **no snmp-server location**

Parameters

Parameters	Description
TEXT	Specifies the string that describes the system location information. The maximum length is 255 characters. The syntax is a general string that allows spaces.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to configure the system's location information on the Switch.

Example

This example shows how to configure the system's location information with the string "HQ 15F".

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server location HQ 15F
GA-MLxxTPoE+(config)#
```

9.1.17 snmp-server name

This command is used to configure the system's name information. Use the **no** form of this command to remove the setting.

Syntax

- **snmp-server name** *NAME*
- **no snmp-server name**

Parameters

Parameters	Description
NAME	Specifies the string that describes the host name information. The maximum length is 255 characters.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to configure the system's name information on the Switch.

Example

This example shows how to configure the system's name to "SiteA-switch".

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server name SiteA-switch
GA-MLxxTPoE+(config)#
```

9.1.18 snmp-server trap-sending disable

This command is used to disable the port's trap sending state. Use the **no** form of this command to enable the port's trap sending state.

Syntax

- **snmp-server trap-sending disable**
- **no snmp-server trap-sending disable**

Parameters

None

Default

By default, this option is enabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to disable the port to send SNMP notification traps out of the configured port. If the sending is disabled, then SNMP notification traps generated by the system are not allowed to transmit out of the port. The SNMP traps generated by other system and forwarded to the port is not subject to this restriction.

Example

This example shows how to disable the sending of the notification traps out of GigabitEthernet1/0/8.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/8
GA-MLxxTPoE+(config-if)# snmp-server trap-sending disable
GA-MLxxTPoE+(config-if)#
```

9.1.19 snmp-server service-port

This command is used to configure the SNMP UDP port number. Use the **no** form of this command to revert to the default setting.

Syntax

- **snmp-server service-port** *PORT-NUMBER*
- **no snmp-server service-port**

Parameters

Parameters	Description
PORT-NUMBER	Specifies the UDP port number. The range is from 1 to 65535. Some numbers may conflict with other protocols.

Default

By default, this number is 161.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to configure the SNNP UDP port number on the Switch. The agent will listen to the SNMP request packets on the configured service UDP port number.

Example

This example shows how to configure the SNMP UDP port number.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server service-port 50000
GA-MLxxTPoE+(config)#
```

9.1.20 snmp-server response broadcast-request

This command is used to enable the server to response to broadcast SNMP GetRequest packets. Use the **no** form of this command to disable the response to broadcast SNMP GetRequest packets.

Syntax

- **snmp-server response broadcast-request**
- **no snmp-server response broadcast-request**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to enable or disable the server to response to broadcast SNMP GetRequest packet. NMS tools would send broadcast SNMP GetRequest packets to discover networks device. To support this function, the response to the broadcast get request packet needs to be enabled.

Example

This example shows how to enable the server to respond to the broadcast SNMP get request packet.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server response broadcast-request
GA-MLxxTPoE+(config)#
```

9.1.21 snmp trap link-status

This command is used to enable the notification of link-up and link-down events that occurred on the interface. Use the **no** form of this command to disable the notification.

Syntax

- **snmp trap link-status**
- **no snmp trap link-status**

Parameters

None

Default

By default, this option is enabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to enable or disable the sending of link-up and link-down traps on an interface.

Example

This example shows how to disable the generation of link-up and link-down traps on GigabitEthernet1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# no snmp trap link-status
GA-MLxxTPoE+(config-if)#
```

9.2 LLDP (Link Layer Discovery Protocol) Commands

LLDP (Link Layer Discovery Protocol) is a function to periodically collect connected device information. If devices, such as an IP phone, printer, and network camera, support LLDP, you can learn what devices are connected where. This function also allows you to identify configuration errors based on collected information and change the protocol settings or switch operations according to the information.

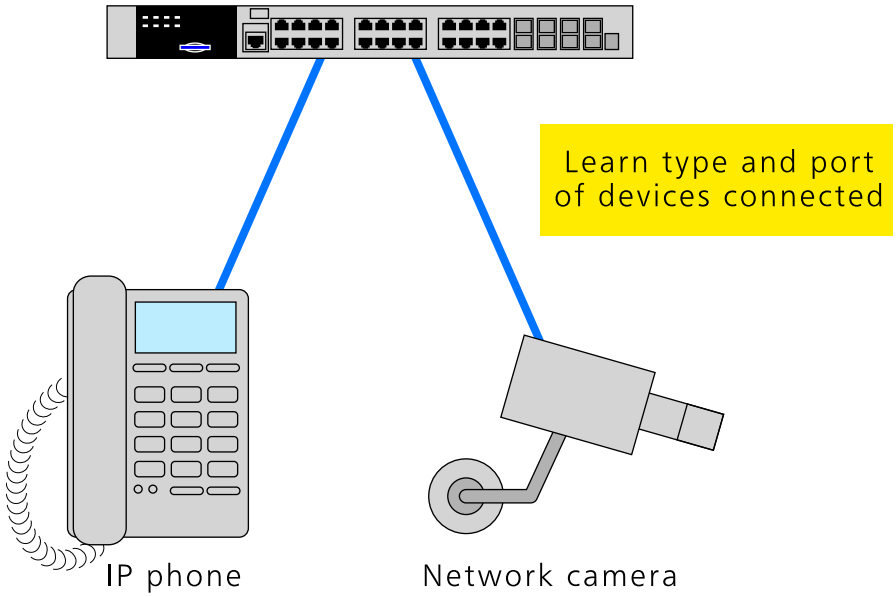


Figure 58-1 LLDP overview

9.2.1 clear lldp counters

This command is used to delete LLDP statistics.

Syntax

- **clear lldp counters** [**all** | **interface** *INTERFACE-ID* [**,** | **-**]]

Parameters

Parameters	Description
all	(Optional) Specifies to clear LLDP counter information for all interfaces and global LLDP statistics.
interface *INTERFACE-ID*	(Optional) Specifies the interface to clear LLDP counter information. Valid interfaces are physical interfaces.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

Use this command with the **interface** keyword to reset LLDP statistics of the specified interface(s). If the command **clear lldp counters** is issued with the **all** keyword to clear global LLDP statistics and the LLDP statistics on all interfaces. When no optional parameter is configured, only the LLDP global counters will be cleared.

Example

This example shows how to clear all LLDP statistics.

```
GA-MLxxTPoE+# clear lldp counters all
GA-MLxxTPoE+#
```

9.2.2 clear lldp table

This command is used to delete all LLDP information learned from neighboring devices.

Syntax

- **clear lldp table {all | interface** *INTERFACE-ID* **[, | -]}**

Parameters

Parameters	Description
all	Specifies to clear LLDP neighboring information for all interfaces.
INTERFACE-ID	Specifies the interface ID. Valid interfaces are physical interfaces.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

If this command is issued without the **interface** keyword, all neighboring information on all interfaces will be cleared.

Example

This example shows how to clear all neighboring information on all interfaces.

```
GA-MLxxTPoE+# clear lldp table all
GA-MLxxTPoE+#
```

9.2.3 lldp dot1-tlv-select

This command is used to specify which optional type-length-value settings (TLVs) in the IEEE 802.1 organizationally specific TLV set will be transmitted and encapsulated in LLDPDUs, and sent to neighbor devices. Use the **no** form of this command to disable the transmission of TLVs.

Syntax

- **lldp dot1-tlv-select** {**port-vlan** | **protocol-vlan** *VLAN-ID* [**,** | **-**] | **vlan-name** [*VLAN-ID* [**,** | **-**]] | **protocol-identity** [*PROTOCOL-NAME*]}
- **no lldp dot1-tlv-select** {**port-vlan** | **protocol-vlan** [*VLAN-ID* [**,** | **-**]] | **vlan-name** [*VLAN-ID* [**,** | **-**]] | **protocol-identity** [*PROTOCOL-NAME*]}

Parameters

Parameters	Description
port-vlan	Specifies the port VLAN ID TLV to send. The Port VLAN ID TLV is an optional fixed length TLV that allows a VLAN bridge port to advertise the port VLAN identifier (PVID) that will be associated with untagged or priority tagged frames.
protocol-vlan	Specifies the Port and Protocol VLAN ID (PPVID) TLV to send. The PPVID TLV is an optional TLV that allows a bridge port to advertise a port and protocol VLAN ID.
VLAN-ID	Specifies the ID of the VLAN in the PPVID TLV. The VLAN ID range is 1 to 4094. If no VLAN ID is specified, all configured PPVID VLANs will be cleared and no PPVID TLV will be sent.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.
vlan-name	Specifies the VLAN name TLV to send. The VLAN name TLV is an optional TLV that allows an IEEE 802.1Q-compatible IEEE 802 LAN station to advertise the assigned name of any VLAN with which it is configured.
VLAN-ID	(Optional) Specifies the ID of the VLAN in the VLAN name TLV. The VLAN ID range is 1 to 4094. If no VLAN ID is specified, all configured VLANs for the VLAN name TLV will be cleared and no VLAN name TLV will be sent.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.

Parameters	Description
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.
protocol-identity	Specifies the Protocol Identity TLV to send. The Protocol Identity TLV is an optional TLV that allows an IEEE 802 LAN station to advertise particular protocols that are accessible through the port.
PROTOCOL-NAME	(Optional) Specifies the protocol name here. The valid strings for *PROTOCOL-NAME* are: **eapol** - Extensible Authentication Protocol (EAP) over LAN **lacp** - Link Aggregation Control Protocol **gvrp** - GARP VLAN Registration Protocol **stp** - Spanning Tree Protocol

Default

No IEEE 802.1 organizationally specific TLV is selected.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is available for physical port configurations. If the optional TLVs advertisement state is enabled, they will be encapsulated in LLDPDUs and sent to other devices.
The protocol identity TLV optional data type indicates whether to advertise the corresponding local system protocol identity instance on the port. The protocol identity TLV provides a way for devices to advertise protocols that are important to the operation of the network. For example, protocols like Spanning Tree Protocol, Link Aggregation Control Protocol, and numerous vendor proprietary variations are responsible for maintaining the topology and connectivity of the network. When both of the protocol functions are working and the protocol identity is enabled for advertising on a port, the protocol identity TLV will be advertised.
Only when the configured VLAN ID matches the configuration of the protocol VLAN on that interface and the VLAN exists, then the PPVID TLV for that VLAN will be sent. Only when the interface is a member port of the configured VLAN ID, the VLAN will be advertised in VLAN Name TLV.

Example

This example shows how to enable advertising Port VLAN ID TLV.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# lldp dot1-tlv-select port-vlan
GA-MLxxTPoE+(config-if)#
```

This example shows how to enable advertising Port and Protocol VLAN ID TLV. The advertised VLAN includes 1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# lldp dot1-tlv-select protocol-vlan 1
GA-MLxxTPoE+(config-if)#
```

This example shows how to enable the VLAN Name TLV advertisement from vlan1 to vlan3.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#lldp dot1-tlv-select vlan-name 1-3
GA-MLxxTPoE+(config-if)#
```

This example shows how to enable the STP Protocol Identity TLV advertisement.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# lldp dot1-tlv-select protocol-identify stp
GA-MLxxTPoE+(config-if)#
```

9.2.4 lldp dot3-tlv-select

This command is used to specify which optional type-length-value settings (TLVs) in the IEEE 802.3 organizationally specific TLV set will be encapsulated in LLDPDUs and sent to neighbor devices. Use the **no** form of this command to disable the transmission of the TLVs.

Syntax

- **lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | max-frame-size | power-via-mdi]**
- **no lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | max-frame-size | power-via-mdi]**

Parameters

Parameters	Description
mac-phy-cfg	(Optional) Specifies the MAC/PHY configuration/status TLV to send. The MAC/PHY configuration/status TLV is an optional TLV that identifies (1) the duplex and bit-rate capability of the sending IEEE 802.3 LAN node, and (2) the current duplex and bit-rate settings of the sending IEEE 802.3 LAN node.
link-aggregation	(Optional) Specifies the link aggregation TLV to send. The link aggregation TLV contains the following information. Whether the link is capable of being aggregated, whether the link is currently in an aggregation, and the aggregated port channel ID of the port. If the port is not aggregated, then the ID is 0.
max-frame-size	(Optional) Specifies the maximum frame size TLV to send. The maximum frame size TLV indicates the maximum frame size capability of the implemented MAC and PHY.
power-via-mdi	Enable transmission of the MDI TLV
power-via-mdimeasurements	Enable transmission of the MDI Measurements TLV

Default

No IEEE 802.3 organizationally specific TLV is selected.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is available for physical port configuration. This command enables the advertisement of the optional IEEE 802.3 organizationally specific TLVs. The respective TLV will be encapsulated in LLDPDU and sent to other devices if the advertisement state is enabled.
When no optional parameter is specified, all supported IEEE 802.3 organizationally specific TLVs are selected or de-selected in this command.

Example

This example shows how to enable the advertising MAC/PHY Configuration/ Status TLV.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# lldp dot3-tlv-select mac-phy-cfg
GA-MLxxTPoE+(config-if)#
```

9.2.5 lldp fast-count

This command is used to configure the LLDP-MED fast start repeat count option on the Switch. Use the **no** form of this command to revert to the default setting.

Syntax

- **lldp fast-count** *VALUE*
- **no lldp fast-count** *VALUE*

Parameters

Parameters	Description
VALUE	Specifies the LLDP-MED fast start repeat count value. This value must be between 1 and 10.

Default

By default, this value is 4.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

When an LLDP-MED capabilities TLV is detected, the application layer will start the fast start mechanism. This command is used to configure the fast start repeat count which indicates the number of LLDP message transmissions for one complete fast start interval.

Example

This example shows how to configure the LLDP MED fast start repeat count.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# lldp fast-count 10
GA-MLxxTPoE+(config)#
```

9.2.6 lldp hold-multiplier

This command is used to configure the hold multiplier for LLDP updates on the Switch. Use the **no** form of this command to revert to the default setting.

Syntax

- **lldp hold-multiplier** *VALUE*

Parameters

Parameters	Description
VALUE	Specifies the multiplier on the LLDPDU transmission interval that used to compute the TTL value of an LLDPDU. This value must be between 2 and 10.

Default

By default, this value is 4.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This parameter is a multiplier on the LLDPDU transmission interval that is used to compute the TTL value in an LLDPDU. The lifetime is determined by the hold-multiplier times the TX-interval. At the partner switch, when the TTL for a given advertisement expires, the advertised data is deleted from the neighbor switch's MIB.

Example

This example shows how to configure the LLDP hold-multiplier to 3.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# lldp hold-multiplier 3
GA-MLxxTPoE+(config)#
```

9.2.7 lldp management-address

This command is used to configure the management address that will be advertised on the physical interface. Use the **no** form of this command to remove the settings.

Syntax

- **lldp management-address** [*IP-ADDRESS* | *IPV6-ADDRESS*]
- **no lldp management-address** [*IP-ADDRESS* | *IPV6-ADDRESS*]

Parameters

Parameters	Description
IP-ADDRESS	(Optional) Specifies the IPv4 address that is carried in the management address TLV.
IPV6-ADDRESS	(Optional) Specifies the IPv6 address that is carried in the management address TLV.

Default

No LLDP management address is configured (no Management Address TLV is sent).

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is available for physical port configuration. This command specifies the IPv4/IPv6 address that is carried in the management address TLV on the specified port. If an IP address is specified, but the address is not associated with one of the interfaces on the system, then the address will not be sent.
When no address is specified using the **lldp management-address** command, the Switch will find at least one IPv4 and IPv6 address in the VLAN with the lowest VLAN ID. If no applicable IPv4/IPv6 address exists, then no management address TLV will be advertised. Once the administrator configures an address, both of the default IPv4 and IPv6 management address will become inactive and will not be sent. The default IPv4 or IPv6 address will be active again when all the configured addresses are removed. Multiple IPv4/IPv6 management addresses can be configured by using this command multiple times.
Use the **no lldp management-address** command without a management address to disable the management address adverted in LLDPDUs. If there is no effective management address in the list, no management address TLV will be sent.

Example

This example shows how to enable GigabitEthernet1/0/1 and 1/0/2 for setting the management address entry (IPv4).

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface range gi1/0/1-1/0/2
GA-MLxxTPoE+(config-if-range)# lldp management-address 10.1.1.1
GA-MLxxTPoE+(config-if-range)#
```

This example shows how to enable GigabitEthernet1/0/3 and 1/0/4 for setting the management address entry (IPv6).

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface range gi1/0/3-1/0/4
GA-MLxxTPoE+(config-if-range)# lldp management-address FE80::250:A2FF:FEBF:A056
GA-MLxxTPoE+(config-if-range)#
```

This example shows how to delete the management address 10.1.1.1 from GigabitEthernet1/0/1 and 1/0/2. If 10.1.1.1 is the last one, no management address TLV will be sent.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface range gi1/0/1-1/0/2
GA-MLxxTPoE+(config-if-range)# no lldp management-address 10.1.1.1
GA-MLxxTPoE+(config-if-range)#
```

This example shows how to delete the management address FE80::250:A2FF:FEBF:A056 from GigabitEthernet1/0/3. and 1/0/4.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface range gi1/0/3-1/0/4
GA-MLxxTPoE+(config-if-range)# no lldp management-address FE80::250:A2FF:FEBF:A056
GA-MLxxTPoE+(config-if-range)#
```

This example shows how to delete all management addresses from GigabitEthernet1/0/5 and then no management address TLV will be sent on GigabitEthernet1/0/5.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/5
GA-MLxxTPoE+(config-if)# no lldp management-address
GA-MLxxTPoE+(config-if)#
```

9.2.8 lldp med-tlv-select

This command is used to specify which optional LLDP-MED TLV will be transmitted and encapsulated in the LLDPDUs and sent to neighbor devices. Use the **no** form of this command to disable the transmission of the TLVs.

Syntax

- **lldp med-tlv-select [capabilities | inventory-management | network-policy]**
- **no lldp med-tlv-select [capabilities | inventory-management | network-policy]**

Parameters

Parameters	Description
capabilities	(Optional) Specifies to transmit the LLDP-MED capabilities TLV.
inventory-management	(Optional) Specifies to transmit the LLDP-MED inventory management TLV.
network-policy	(Optional) Specifies to transmit the LLDP-MED network policy TLV.

Default

No LLDP-MED TLV is selected.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is available for physical port configuration. This command is used to enable or disable transmitting LLDP-MED TLVs.
When disabling the transmission of the capabilities TLV, LLDP-MED on the physical interface will be disabled at the same time. In other words, all LLDP-MED TLVs will not be sent, even when other LLDP-MED TLVs are enabled.
By default, the Switch only sends LLDP packets until it receives LLDP-MED packets from the end device. The Switch continues to send LLDP-MED packets until it receives LLDP packets only.

Example

This example shows how to enable transmitting LLDP-MED TLVs and LLDP-MED Capabilities TLVs.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# lldp med-tlv-select capabilities
GA-MLxxTPoE+(config-if)#
```

9.2.9 lldp receive

This command is used to enable a physical interface to receive LLDP messages. Use the **no** form of this command to disable receiving LLDP messages.

Syntax

- **lldp receive**
- **no lldp receive**

Parameters

None

Default

LLDP is enabled on all supported interfaces.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is available for physical port configuration. This command is used to enable a physical interface to receive LLDP messages. When LLDP is not running, the Switch does not receive LLDP messages.

Example

This example shows how to enable a physical interface to receive LLDP messages.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# lldp receive
GA-MLxxTPoE+(config-if)#
```

9.2.10 lldp reinit

This command is used to configure the minimum re-initialization the delay on the Switch. Use the **no** form of this command to revert to the default setting.

Syntax

- **lldp reinit** *SECONDS*

Parameters

Parameters	Description
SECONDS	Specifies the delay value for LLDP initialization on an interface. This value must be between 1 and 10 seconds.

Default

By default, this value is 2 seconds.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

A re-enabled LLDP physical interface will wait for the re-initialization delay after the last disable command before reinitializing.

Example

This example shows how to configure the re-initialization delay interval to 5 seconds.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# lldp reinit 5
GA-MLxxTPoE+(config)#
```

9.2.11 lldp run

This command is used to enable the LLDP globally. Use the **no** form of this command to revert to the default setting.

Syntax

- **lldp run**
- **no lldp run**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to globally enable LLDP so that the Switch can start to transmit LLDP packets and receive and process the LLDP packets. The transmission and receiving of LLDP can be controlled respectively by the **lldp transmit** command and the **lldp receive** command in the Interface Configuration mode. LLDP takes effect on a physical interface only when it is enabled both globally and on the physical interface.
By advertising LLDP packets, the Switch announces the information to its neighbor through physical interfaces. The Switch will learn the connectivity and management information from the LLDP packets advertised from the neighbor(s).

Example

This example shows how to enable LLDP.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# lldp run
GA-MLxxTPoE+(config)#
```

9.2.12 lldp forward

This command is used to enable the LLDP forwarding state. Use the **no** form of this command to revert to the default setting.

Syntax

- **lldp forward**
- **no lldp forward**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This is a global control for the LLDP forward. When the LLDP global state is disabled and LLDP forwarding is enabled, the received LLDPDU packet will be forwarded.

Example

This example shows how to enable the LLDP global forwarding state.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# lldp forward
GA-MLxxTPoE+(config)#
```

9.2.13 lldp tlv-select

This command is used to select the TLVs in the 802.1AB basic management set and will be transmitted and encapsulated in the LLDPDUs and sent to neighbor devices. Use the **no** form of this command to revert to the default setting.

Syntax

- **lldp tlv-select [port-description | system-capabilities | system-description | system-name]**
- **no lldp tlv-select [port-description | system-capabilities | system-description | system-name]**

Parameters

Parameters	Description
port-description	(Optional) Specifies the port description TLV to send. The port description TLV allows for the IEEE 802 LAN station's port description to be advertised.
system-capabilities	(Optional) Specifies the system capabilities TLV to send. The system capabilities field will contain a bit-map of the capabilities that defines the primary functions of the system.
system-description	(Optional) Specifies the system description TLV to send. The system description should include the full name and version identification of the system's hardware type, software operating system, and networking software.

Parameters	Description
system-name	(Optional) Specifies the system name TLV to send. The system name should be the system's fully qualified domain name.

Default

No optional 802.1AB basic management TLV is selected.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is available for physical port configuration. This command is used to select the optional TLVs to be transmitted. If the optional TLVs advertisement is selected, they will be encapsulated in the LLDPDU and sent to other devices.

Example

This example shows how to enable all supported optional 802.1AB basic management TLVs.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# lldp tlv-select
GA-MLxxTPoE+(config-if)#
```

This example shows how to enable advertising the system name TLV.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# lldp tlv-select system-name
GA-MLxxTPoE+(config-if)#
```

9.2.14 lldp transmit

This command is used to enable the LLDP advertise (transmit) capability. Use the **no** form of this command to disable LLDP transmission.

Syntax

- lldp transmit
- no lldp transmit

Parameters

None

Default

LLDP transmit is enabled on all supported interfaces.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is available for physical port configuration. This command is used to enable LLDP transmission on a physical interface. When LLDP is not running, the Switch does not transmit LLDP messages.

Example

This example shows how to enable LLDP transmission.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# lldp transmit
GA-MLxxTPoE+(config-if)#
```

9.2.15 lldp tx-delay

This command is used to configure the transmission delay timer. This delay timer defines the minimum interval between the sending of LLDP messages due to constantly changing MIB content. Use the no form of this command to revert to the default setting.

Syntax

- lldp tx-delay *SECONDS*

Parameters

Parameters	Description
SECONDS	Specifies the delay value for sending successive LLDPDUs on an interface. The valid values are from 1 to 8192 seconds and should not be greater than one-fourth of the transmission interval timer.

Default

By default, this value is 2 seconds.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The LLDP transmission interval must be greater than or equal to four times of the transmission delay timer.

Example

This example shows how to configure the transmission delay timer to 8 seconds.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# lldp tx-delay 8
GA-MLxxTPoE+(config)#
```

9.2.16 lldp tx-interval

This command is used to configure the LLDPDUs transmission interval on the Switch. Use the no form of this command to revert to the default setting.

Syntax

- lldp tx-interval *SECONDS*

Parameters

Parameters	Description
SECONDS	Specifies the interval between consecutive transmissions of LLDP advertisements on each physical interface. The range is from 5 to 32768 seconds.

Default

By default, this value is 30 seconds.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This interval controls the rate at which LLDP packets are sent.

Example

This example shows how to configure LLDP updates to be sent every 50 seconds.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# lldp tx-interval 50
GA-MLxxTPoE+(config)#
```

9.2.17 snmp-server enable traps lldp

This command is used to enable the LLDP and LLDP-MED trap state. Use the **no** form of this command disable this feature.

Syntax

- **snmp-server enable traps lldp [med]**
- **no snmp-server enable traps lldp [med]**

Parameters

Parameters	Description
med	(Optional) Specifies to enable the LLDP-MED trap state.

Default

The LLDP and LLDP-MED trap states are disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use the **snmp-server enable traps lldp** command to enable the sending of LLDP notifications.
Use the **snmp-server enable traps lldp med** command to enable the sending of LLDP-MED notifications.

Example

This example shows how to enable the LLDP MED trap.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server enable traps lldp med
GA-MLxxTPoE+(config)#
```

9.2.18 lldp notification enable

This command is used to enable the sending of LLDP and LLDP-MED notifications for the interface. Use the **no** form of this command disable this feature.

Syntax

- **lldp [med] notification enable**
- **no lldp [med] notification enable**

Parameters

Parameters	Description
med	(Optional) Specifies to enable the LLDP-MED notification state.

Default

The LLDP and LLDP-MED notification states are disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use the **lldp notification enable** command to enable the sending of LLDP notifications.
Use the **lldp med notification enable** command to enable the sending of LLDP-MED notifications.

Example

This example shows how to enable the sending of LLDP MED notifications for GigabitEthernet1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# lldp med notification enable
GA-MLxxTPoE+(config-if)#
```

9.2.19 lldp subtype

This command is used to configure the subtype of LLDP TLV(s).

Syntax

- **lldp subtype port-id {mac-address | local}**

Parameters

Parameters	Description
port-id	Specifies the subtype of the port ID TLV.
mac-address	Specifies the subtype of the port ID TLV as "MAC Address (3)" and the field of "port ID" to be encoded with the MAC address.
local	Specifies the subtype of the port ID TLV as "Locally assigned (7)" and the field of "port ID" to be encoded with the port number.

Default

The subtype of port ID TLV is local (port number).

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to specify the subtype of LLDP TLV(s). A port ID subtype is used to indicate how the port is being referenced in the port ID field.

Example

This example shows how to configure the subtype of the port ID TLV to mac-address.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# lldp subtype port-id mac-address
GA-MLxxTPoE+(config-if)#
```

9.2.20 show lldp

This command is used to display the general LLDP configuration of the Switch.

Syntax

- show lldp

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command is used to display the LLDP global configuration of the Switch.

Example

This example shows how to display the LLDP global configuration of the Switch.

```
GA-MLxxTPoE+#show lldp

LLDP System Information
    Chassis ID Subtype        : MAC Address
    Chassis ID                : 00-50-40-xx-xx-xx
    System Name               :
    System Description        : Gigabit Ethernet Switch
    System Capabilities Supported: Repeater, Bridge
    System Capabilities Enabled  : Repeater, Bridge
LLDP-MED System Information:
    Device Class              : Network Connectivity Device
    Hardware Revision         : A1
    Firmware Revision         : V1.0.0.06
    Software Revision         : V2.0.0.00
    Serial Number             : 73Sxxxxxxxx
    Manufacturer Name         : Panasonic
    Model Name                : GA-MLxxTPoE+
    Asset ID                  :

LLDP Configurations
    LLDP State                : Disabled
    LLDP Forward State        : Disabled
    Message TX Interval       : 30
    Message TX Hold Multiplier: 4
    ReInit Delay              : 2

--More--
```

9.2.21 show lldp interface

This command is used to display the LLDP configuration on the physical interface.

Syntax

- **show lldp interface** *INTERFACE-ID* [, | -]

Parameters

Parameters	Description
INTERFACE-ID	Specifies to the interface ID to be displayed. Valid interfaces are physical interfaces.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command displays the LLDP information of each physical interface.

Example

This example shows how to display a specific physical interface's LLDP configuration.

```
GA-MLxxTPoE+#show lldp interface gi1/0/1

Port ID: Gi1/0/1
------------------------------------------------------------------------------
Port ID                                                    :Gi1/0/1
Admin Status                                               :TX and RX
Notification                                               :Disabled
Basic Management TLVs:
    Port Description                                       :Disabled
    System Name                                            :Disabled
    System Description                                     :Disabled
    System Capabilities                                    :Disabled
    Enabled Management Address:
        (None)
IEEE 802.1 Organizationally Specific TLVs:

    Port VLAN ID                                           :Disabled
    Enabled Port_and_Protocol_VLAN_ID
        (None)
    Enabled VLAN Name
        (None)
    Enabled Protocol_Identity
        (None)
IEEE 802.3 Organizationally Specific TLVs:

 --More--
```

Display Parameters

Parameters	Description
Enabled Management Address	Displays the enabled IPv4/IPv6 addresses. '(None)' means that the user did not configure the management address with the **lldp management-address** command or the enabled default IPv4 and IPv6 addresses are not applicable.
Enabled Port and Protocol VLAN ID	Displays enabled port and protocol VLANs. The VLAN list is the configured and enabled VLANs. If there is no configured PPVID VLAN, '(None)' is displayed.
Enabled VLAN Name	Displayed enabled VLANs for sending VLAN Name TLVs. The VLAN list includes the configured and enabled VLANs. If there is no configured VLAN for the VLAN Name TLV, '(None)' is displayed.
Enabled Protocol Identity	Displays the enabled protocol string for protocol identity TLVs. If there is no enabled protocol for the protocol identity TLV, '(None)' is displayed.

9.2.22 show lldp local interface

This command is used to display physical interface information that will be carried in the LLDP TLVs and sent to neighbor devices.

Syntax

- **show lldp local interface** *INTERFACE-ID* **[, | -] [brief | detail]**

Parameters

Parameters	Description
INTERFACE-ID	Specifies the interface ID. Valid interfaces are physical interfaces.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
brief	(Optional) Specifies to display the information in brief mode.
detail	(Optional) Specifies to display the information in detailed mode. If neither brief nor detail is specified, display the information in the normal mode.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command displays each physical interface's local LLDP information currently available for populating outbound LLDP advertisements.

Example

This example shows how to display the local information of port 1 in detailed mode.

```
GA-MLxxTPoE+#show lldp local interface gi1/0/1 detail

Port ID: Gi1/0/1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : Gi1/0/1
Port Description                         : Panasonic GA-MLxxTPoE+ HW A1
                                           firmware V1.0.0.00 Port 1 on Unit 1
Port PVID                                : 1
Management Address Count                 : 2

    Address 1 : (default)
        Subtype                          : IPv4
        Address                          : 192.168.70.124
        IF Type                          : IfIndex
        OID                              : 1.3.6.1.4.1.396.5.4.1.40

    Address 2 :
        Subtype                          : IPv4
        Address                          : 192.168.70.124
        IF Type                          : IfIndex
        OID                              : 1.3.6.1.4.1.396.5.4.1.40

PPVID Entries Count                      : 0
    (None)
--More--
```

This example shows how to display the local information of port 1 in normal mode.

```
GA-MLxxTPoE+#show lldp local interface gi1/0/1

Port ID: Gi1/0/1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : Gi1/0/1
Port Description                         : Panasonic GA-MLxxTPoE+ HW A1
                                           firmware V1.0.0.00 Port 1 on Unit 1
Port PVID                                : 1
Management Address Count                 : 1
PPVID Entries Count                      : 0
VLAN Name Entries Count                  : 1
Protocol Identity Entries Count          : 0
MAC/PHY Configuration/Status             : (See Detail)
Link Aggregation                         : (See Detail)
Maximum Frame Size                       : 1518
LLDP-MED capabilities                    : (See Detail)
Network Policy                           : (See Detail)


GA-MLxxTPoE+#
```

This example shows how to display local information of port 1 in brief mode.

```
GA-MLxxTPoE+#show lldp local interface gi1/0/1 brief

Port ID: Gi1/0/1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : Gi1/0/1
Port Description                         : Panasonic GA-MLxxTPoE+ HW A1
                                           firmware V1.0.0.00 Port 1 on Unit 1


GA-MLxxTPoE+#
```

9.2.23 show lldp management-address

This command is used to display the management address information.

Syntax

- **show lldp management-address** [*IP-ADDRESS* | *IPV6-ADDRESS*]

Parameters

Parameters	Description
IP-ADDRESS	(Optional) Specifies to display the LLDP management information for a specific IPv4 address.
IPV6-ADDRESS	(Optional) Specifies to display the LLDP management information for a specific IPv6 address.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command is used to display the management address information.

Example

This example shows how to display all management address information.

```
GA-MLxxTPoE+#show lldp management-address

Address 1 : (default)
-----------------------------------------------
    Subtype                          : IPv4
    IF Type                          : IfIndex
    OID                              : 1.3.6.1.4.1.396.5.4.1.47
    Advertising Ports                : -

Total Entries : 1
GA-MLxxTPoE+#
```

9.2.24 show lldp neighbor interface

This command is used to display the information currently learned from the neighbor on the specific physical interface.

Syntax

- **show lldp neighbors interface** *INTERFACE-ID* **[, | -] [brief | detail]**

Parameters

Parameters	Description
INTERFACE-ID	Specifies the interface ID. Valid interfaces are physical interfaces.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
brief	(Optional) Specifies to display the information in brief mode.
detail	(Optional) Specifies to display the information in detailed mode. If neither brief nor detail is specified, display the information in normal mode.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command display the information learned from the neighbor devices.

Example

This example shows how to display information about neighboring devices learned by LLDP on GigabitEthernet1/0/9 in detailed mode.

```
GA-MLxxTPoE+#show lldp neighbors interface gi1/0/9 detail

Port ID: Gi1/0/9
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                          : MAC Address
    Chassis ID                                  : 00-50-40-xx-xx-xx
    Port ID Subtype                             : Local
    Port ID                                     : Gi1/0/7
    Port Description                            :
    System Name                                 :
    System Description                          :
    System Capabilities                         :
    Management Address Count                    : 0
        (None)

    Port PVID                                   : 0
    PPVID Entries Count                         : 0
        (None)

    VLAN Name Entries Count                     : 0
        (None)

    Protocol ID Entries Count                   : 0
        (None)

    MAC/PHY Configuration/Status                : (None)
    Power Via MDI                               : (None)
    Link Aggregation                            : (None)
    Maximum Frame Size                          : 0
    Unknown TLVs Count                          : 0
        (None)

        LLDP-MED Capabilities Enabled:
            Capabilities                  : Not Support
            Network Policy                : Not Support
            Location Identification       : Not Support
            Extended Power Via MDI        : Not Support
            Inventory                     : Not Support


    Inventory Management:
        None


GA-MLxxTPoE+#
```

This example shows how to display remote LLDP information in the normal mode.

```
GA-MLxxTPoE+#show lldp neighbor interface gi1/0/1

Port ID: Gi1/0/1
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                          : MAC Address
    Chassis ID                                  : 00-50-40-xx-xx-xx
    Port ID Subtype                             : Local
    Port ID                                     : Gi1/0/1
    Port Description                            : Panasonic GA-MLxxTPoE+ HW ES2 firm
ware V1.0.0.00 Port 1 on Unit 1
    System Name                                 :
    System Description                          :
    System Capabilities                         :
    Management Address Count                    : 0
    Port PVID                                   : 1
    PPVID Entries Count                         : 0
    VLAN Name Entries Count                     : 0
    Protocol ID Entries Count                   : 0
    MAC/PHY Configuration/Status                : (None)
    Power Via MDI                               : (None)
    Link Aggregation                            : (None)
    Maximum Frame Size                          : 0
    LLDP-MED capabilities                       : (None)
    Extended power via MDI                      : (None)
    Network policy                              : (None)
    Inventory Management                        : (None)
    Unknown TLVs Count                          : 0

GA-MLxxTPoE+#
```

This example shows how to display the neighbor information on GigabitEthernet1/0/1 to 1/0/2 in brief mode.

```
GA-MLxxTPoE+# show lldp neighbor interface gi1/0/1-1/0/2 brief

Port ID: Gi1/0/1
------------------------------------------------------------
Remote Entities Count : 2
Entity 1
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-01
      Port ID Subtype               : Local
      Port ID                       : Gi1/0/1
      Port Description              : RMON Port 1 on Unit 3
Entity 2
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-02
      Port ID Subtype               : Local
      Port ID                       : Gi1/0/2
      Port Description              : RMON Port 1 on Unit 4

Port ID : Gi1/0/2
------------------------------------------------------------------------
Remote Entities Count : 3
Entity 1
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-03
      Port ID Subtype               : Local
      Port ID                       : Gi1/0/4
      Port Description              : RMON Port 2 on Unit 1
Entity 2
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-04
      Port ID Subtype               : Local
      Port ID                       : Gi1/0/5
      Port Description              : RMON Port 2 on Unit 2
Entity 3
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-05
      Port ID Subtype               : Local
      Port ID                       : Gi1/0/6
      Port Description              : RMON Port 2 on Unit 3

Total Entries: 2

GA-MLxxTPoE+#
```

9.2.25 show lldp traffic

This command is used to display the system's global LLDP traffic information.

Syntax

- **show lldp traffic**

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

The global LLDP traffic information displays an overview of neighbor detection activities on the Switch.

Example

This example shows how to display global LLDP traffic information.

```
GA-MLxxTPoE+#show lldp traffic

Last Change Time  : 0D0H1M30S
Total Inserts     : 2
Total Deletes     : 0
Total Drops       : 0
Total Ageouts     : 1

GA-MLxxTPoE+#
```

Display Parameters

Parameters	Description
Last Change Time	The amount of time since the last update to the remote table in days, hours, minutes, and seconds.
Total Inserts	Total number of inserts to the remote data table.
Total Deletes	Total number of deletes from the remote data table.
Total Drops	Total number of times that the remote data was received but not inserted due to insufficient resources.
Total Ageouts	Total number of times a complete remote data entry was deleted because the Time to Live interval expired.

9.2.26 show lldp traffic interface

This command is used to display the LLDP traffic information on the specific physical interface.

Syntax

- **show lldp traffic interface** *INTERFACE-ID* **[, | -]**

Parameters

Parameters	Description
INTERFACE-ID	Specifies the interface ID. Valid interfaces are physical interfaces.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command displays LLDP traffic on each physical interface.

Example

This example shows how to display statistics information of port 1.

```
GA-MLxxTPoE+#show lldp traffic interface gi1/0/1

Port ID : Gi1/0/1
-------------------------------------------
    Total Transmits     : 0
    Total Discards      : 0
    Total Errors        : 0
    Total Receives      : 0
    Total TLV Discards  : 0
    Total TLV Unknowns  : 0
    Total Ageouts       : 0

GA-MLxxTPoE+#
```

Display Parameters

Parameters	Description
Total Transmits	The total number of LLDP packets transmitted on the port.
Total Discards	The total number of LLDP frames discarded on the port for any reason.
Total Errors	The number of invalid LLDP frames received on the port.
Total Receives	The total number of LLDP packets received on the port.
Total TLV Discards	The number of TLVs discarded.
Total TLV Unknowns	The total number of LLDP TLVs received on the port where the type value is in the reserved range, and not recognized.
Total Ageouts	The total number of times a complete remote data entry was deleted for the port because the Time to Live interval expired.

9.3 SMTP (Simple Mail Transfer Protocol) Commands

9.3.1 smtp server

This command is used to configure the SMTP server and port setting.

Syntax

- **smtp server** {*IP-ADDRESS* | *IPV6-ADDRESS*} [**port** *PORT*]
- **no smtp server** [**port**]

Parameters

Parameters	Description
IP-ADDRESS	Specifies the IPv4 address of the SMTP server.
IPV6-ADDRESS	Specifies the IPv6 address of the SMTP server.
port *PORT*	Specifies the TCP port number used to contact the SMTP server. The valid range is from 1 and 65535.

Default

By default, no server address is configured.
By default, the port number is 25.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The system provides the service to send SYSLOG messages to email receivers via SMTP. Email messages will only be sent only when the mail server, recipient, and own mail address are configured. The Switch acts as the SMTP client and sends the SYSLOG message to the SMTP server, then the server will delivers email messages to the recipient. Up to one SMTP server can be configured for a switch.

Example

This example shows how to configure the server IP to 172.18.208.9 and the TCP port to 587.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# smtp server 172.18.208.9 port 587
GA-MLxxTPoE+(config)#
```

9.3.2 smtp self

This command is used to configure the email address which represents the Switch that sends the email message. Use the **no** form of this command to remove the self email address.

Syntax

- **smtp self** *EMAIL-ADDRESS*
- **no smtp self**

Parameters

Parameters	Description
self *EMAIL-ADDRESS*	Specifies the email address that which represents the Switch.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to configure the email address that represents the Switch. Only one email address can be configured for this switch.

Example

This example shows how to configure the Switch's email sender address as switch@domain.com.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# smtp self switch@domain.com
GA-MLxxTPoE+(config)#
```

9.3.3 smtp recipient

This command is used to configure the recipient where the email will be sent. Use the **no** form of this command to remove a recipient.

Syntax

- **smtp recipient** *EMAIL-ADDRESS*
- **no smtp recipient** {**all** | *EMAIL-ADDRESS*}

Parameters

Parameters	Description
EMAIL-ADDRESS	Specifies a recipient to receive the email.
all	Specifies all recipients to be removed.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The system provides the service to send SYSLOG messages to email receivers via SMTP. Use the **smtp recipient** command to configure the email address to receive the email message. By default, no messages will be sent. Use the **logging smtp** command to enable the sending of SYSLOG messages to the email recipients and configure the filtering criteria.

Example

This example shows how to add the receiver mail address as receiver@domain.com.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# smtp recipient receiver@domain.com
GA-MLxxTPoE+(config)#
```

9.3.4 smtp interval

This command is used to configure the SMTP interval time. Use the **no** form of this command to revert to the default setting.

Syntax

- **smtp interval** *MINUTES*
- **no smtp interval**

Parameters

Parameters	Description
MINUTES	Specifies the SMTP sending interval. If set to 0, the Switch will send a mail for each event immediately. The valid range is from 0 and 65535.

Default

By default, this value is 30 minutes.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to configure the SMTP sending interval that the Switch uses.

Example

This example shows how to configure the interval to 10 minutes.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# smtp interval 10
GA-MLxxTPoE+(config)#
```

9.3.5 show smtp

This command is used to display SMTP information.

Syntax

- show smtp

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

This command is used to display information of SMTP.

Example

This example shows how to display SMTP information.

```
GA-MLxxTPoE+#show smtp

SMTP IPv4 Server Address: 172.18.208.9
SMTP IPv4 Server Port   : 587
SMTP IPv6 Server Address: 1000::1111
SMTP IPv6 Server Port   : 25
Self Mail Address       : switch@domain.com
Send Interval           : 10

Index    Mail Receiver Address
-----    ------------------------------------------------------------------------
1        receiver@domain.com
2        receiver2@domain.com
3        receiver3@domain.com
4        receiver4@domain.com
5        receiver5@domain.com
6        receiver6@domain.com
7        receiver7@domain.com
8        receiver8@domain.com
GA-MLxxTPoE+#
```

9.3.6 smtp send-testmsg

This command is used to check the reachability of the SMTP server.

Syntax

- smtp send-testmsg

Parameters

None

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to check the reachability of the SMTP server. An email will be sent to all of the configured recipients.

Example

This example shows how to send a test mail to all users currently configured in the recipient list.

```
GA-MLxxTPoE+#smtp send-testmsg

Subject:Test SMTP
Content:This is the text message.

Sending mail, please wait...
GA-MLxxTPoE+#
```

10 IP packet relay and IP additional functions

10.1 DHCP Client Commands

ARP (Address Resolution Protocol) is used to calculate a MAC address from an IP address if the destination MAC address is unknown.
Gratuitous ARP is a special ARP packet sent when an IP interface is booted, sending an inquiry by setting its own IP address instead of the destination IP address. If other device responds to Gratuitous ARP, it means the IP address is duplicated.

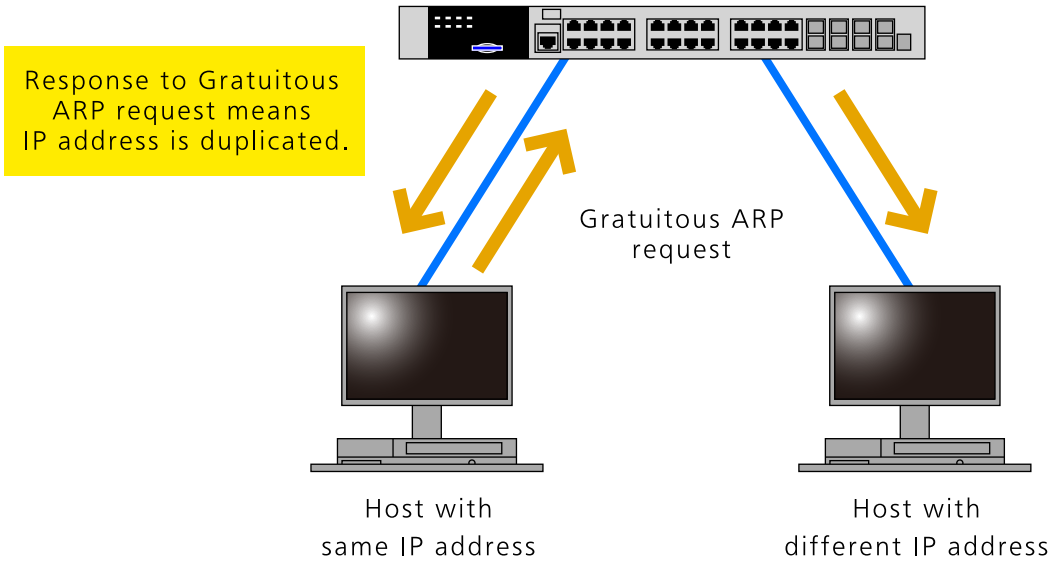


Figure 60-1 Gratuitous ARP overview

10.1.1 ip dhcp client class-id

This command is used to specify the vendor class identifier used as the value of Option 60 for the DHCP discover message. Use the **no** form of this command to revert to the default setting.

Syntax

- **ip dhcp client class-id** {*STRING* | **hex** *HEX-STRING*}
- **no ip dhcp client class-id**

Parameters

Parameters	Description
STRING	Specifies the vendor class identifier in the string form. The maximum length of the string is 32.
HEX-STRING	Specifies a vendor class identifier in the hexadecimal form. The maximum length of the string is 64.

Default

The device type will be used as the class ID.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for VLAN interface configuration.
Use this command to specify a vendor class identifier (Option 60) to be sent with the DHCP discover message. This specification only applies to the subsequent sending of the DHCP discover messages. The setting only takes effect when the DHCP client is enabled on the interface to acquire the IP address from the DHCP server. The vendor class identifier specifies the type of device that is requesting an IP address.

Example

This example shows how to enable the DHCP client, enable the sending of the Vendor Class Identifier, and specifies its value as VOIP-Device for VLAN 100.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface vlan 100
GA-MLxxTPoE+(config-if)# ip address dhcp
GA-MLxxTPoE+(config-if)# ip dhcp client class-id VOIP-Device
GA-MLxxTPoE+(config-if)#
```

10.1.2 ip dhcp client hostname

This command is used to specify the value of the host name option to be sent with the DHCP discover message. Use the **no** form of this command to revert to the default setting.

Syntax

- **ip dhcp client hostname** *HOST-NAME*
- **no ip dhcp client hostname**

Parameters

Parameters	Description
HOST-NAME	Specifies the host name. The maximum length is 64 characters. The host name must start with a letter, end with a letter or digit, and only with interior characters letters, digits, and hyphens.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for VLAN interface configuration.
se this command to specify the host name string (Option 12) to be sent with the DHCP discover message. The specification only applies to the subsequent sending of the DHCP discover messages. The setting only takes effect when the DHCP client is enabled on the interface to acquire the IP address from the DHCP server. If this option is not configured, the name defined by the **snmp-server name** command will be sent as Option 12 with the message.

Example

This example shows how to set the host name option value to Site-A-Switch.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface vlan 100
GA-MLxxTPoE+(config-if)# ip dhcp client hostname Site-A-Switch
GA-MLxxTPoE+(config-if)#
```

10.1.3 ip dhcp client lease

This command is used to specify the preferred lease time for the IP address to request from the DHCP server. Use the **no** form of this command to disable sending of the lease option.

Syntax

- **ip dhcp client lease** *DAYS* [*HOURS* [*MINUTES*]]
- **no ip dhcp client lease**

Parameters

Parameters	Description
DAYS	Specifies the day duration of the lease. The range is from 0 to 10000 days.
HOURS	(Optional) Specifies the hour duration of the lease. The range is from 0 to 23 hours.
MINUTES	(Optional) Specifies the minute duration of the lease. The range is from 0 to 59 minutes.

Default

The lease option is not sent.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for VLAN interface configuration.

The setting only takes effect when the DHCP client is enabled to request the IP address for the interface.

Example

This example shows how to get a 5 days release of the IP address.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface vlan 100
GA-MLxxTPoE+(config-if)# ip address dhcp
GA-MLxxTPoE+(config-if)# ip dhcp client lease 5
GA-MLxxTPoE+(config-if)#
```

10.2 DHCP Snooping Commands

The commands are used to allow only clients with a regular IP address assigned by the DHCP server to communicate.
When this function is enabled, all ports are set to "untrusted." You need to change the DHCP server and DHCP relay ports to "trusted." In communications from clients connected on "untrusted" ports, only DHCP packets are authenticated first and other packets are discarded. The switch monitors communications with the DHCP server on a "trusted" port and stores a mapping between assigned IP addresses and MAC addresses in the Binding Table in the switch.
Only clients with an IP address and MAC address stored in the Binding Table are authorized for normal communication.

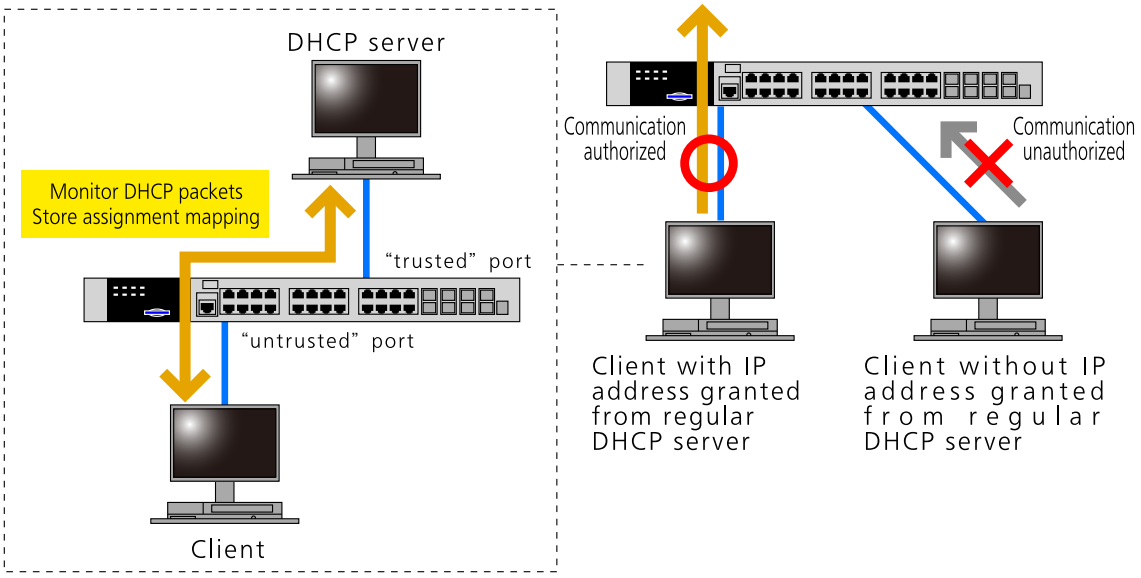


Figure 61-1

10.2.1 ip dhcp snooping

This command is used to globally enable DHCP snooping. Use the **no** form of this command to disable DHCP snooping.

Syntax

- **ip dhcp snooping**

- no ip dhcp snooping

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The DHCP snooping function snoops the DHCP packets arriving at the untrusted interface on the VLAN that is enabled for DHCP snooping. With this function, the DHCP packets that come from the untrusted interface can be validated and a DHCP binding database will be constructed for the DHCP snooping enabled VLAN. The binding database provides IP and MAC binding information that can be further used by the IP source guard and dynamic ARP inspection process.

Example

This example shows how to enable DHCP snooping.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip dhcp snooping
GA-MLxxTPoE+(config)#
```

10.2.2 ip dhcp snooping information option allow-untrusted

This command is used to globally allow DHCP packets with the relay Option 82 on the untrusted interface. Use the **no** form of this command to not allow packets with the relay Option 82.

Syntax

- ip dhcp snooping information option allow-untrusted

- no ip dhcp snooping information option allow-untrusted

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The DHCP snooping function validates the DHCP packets when it arrives at the port on the VLAN that is enabled for DHCP snooping. By default, the validation process will drop the packet if the gateway address is not equal to 0 or Option 82 is present.

Example

This example shows how to enable DHCP snooping for Option 82 to allow untrusted ports.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip dhcp snooping information option allow-untrusted
GA-MLxxTPoE+(config)#
```

10.2.3 ip dhcp snooping database

This command is used to configure the storing of DHCP snooping binding entries to the local flash or a remote site. Use the **no** form of this command to disable the storing or reset the parameters to the default setting.

Syntax

- ip dhcp snooping database {*URL* | write-delay *SECONDS*}
- no ip dhcp snooping database [write-delay]

Parameters

Parameters	Description
URL	Specifies the URL in one of the following forms: • tftp://location/filename • flash:/filename
write-delay *SECONDS*	Specifies the time delay to write the entries after a change is seen in the binding entry. The default is 300 seconds. The range is from 60 to 86400.

Default

By default, the URL for the database agent is not defined.
The write delay value is set to 300 seconds.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to store the DHCP binding entry to local flash or remote server. Use the follow methods to store DHCP binding entries:

- **ftp:** Store the entries to remote site via FTP.
- **tftp:** Store the entries to remote site via TFTP.

The lease time of the entry will not be modified and the live time will continue to be counted while the entry is provisioned.

Example

This example shows how to store the binding entry to a file in the file system.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip dhcp snooping database tftp: //10.0.0.2/store/dhcp-snp-bind
GA-MLxxTPoE+(config)#
```

10.2.4 clear ip dhcp snooping database statistics

This command is used to clear the DHCP binding database statistics.

Syntax

- clear ip dhcp snooping database statistics

Parameters

None

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

When you enter this command, the Switch will clear the database statistics.

Example

This example shows how to clear the snooping database statistics.

```
GA-MLxxTPoE+# clear ip dhcp snooping database statistics
GA-MLxxTPoE+#
```

10.2.5 clear ip dhcp snooping binding

This command is used to clear the DHCP binding entry.

Syntax

- clear ip dhcp snooping binding [*MAC-ADDRESS*] [*IP-ADDRESS*] [vlan *VLAN-ID*] [interface *INTERFACE-ID*]

Parameters

Parameters	Description
MAC-ADDRESS	(Optional) Specifies the MAC address to clear.
IP-ADDRESS	(Optional) Specifies the IP address to clear.

Parameters	Description
vlan *VLAN-ID*	(Optional) Specifies the VLAN ID to clear.
interface *INTERFACE-ID*	(Optional) Specifies the interface to clear.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to clear the DHCP binding entry, including the manually configured binding entry.

Example

This example shows how to clear all snooping binding entries.

```
GA-MLxxTPoE+# clear ip dhcp snooping binding
GA-MLxxTPoE+#
```

10.2.6 renew ip dhcp snooping database

This command is used to renew the DHCP binding database.

Syntax

- **renew ip dhcp snooping database** *URL*

Parameters

Parameters	Description
URL	Specifies load the bind entry database from the URL and add the entries to the DHCP snooping binding entry table. The URL format can be: • ftp://username:password@location:tcpport/filename • tftp://location/filename

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

Using this command will cause the system to load the bind entry database from a URL and add the entries to the DHCP snooping binding entry table.

Example

This example shows how to renew the DHCP snooping binding database.

```
GA-MLxxTPoE+# renew ip dhcp snooping database tftp: //10.0.0.2/store/dhcp-snp-bind
GA-MLxxTPoE+#
```

10.2.7 ip dhcp snooping binding

This command is used to manually configure a DHCP snooping entry.

Syntax

- **ip dhcp snooping binding** *MAC-ADDRESS* **vlan** *VLAN-ID IP-ADDRESS* **interface** *INTERFACE-ID* **expiry** *SECONDS*

Parameters

Parameters	Description
MAC-ADDRESS	Specifies the MAC address of the entry to add or delete.
vlan *VLAN-ID*	Specifies the VLAN of the entry to add or delete.
IP-ADDRESS	Specifies the IP address of the entry to add or deleted.
interface *INTERFACE-ID*	Specifies the interface (physical port and port channel) on which to add or delete a binding entry.
expiry *SECONDS*	Specifies the interval after which bindings are no longer valid. This value must be between 60 and 4294967295 seconds.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to create a dynamic DHCP snooping entry.
To successfully create DHCP snooping entries:

- DHCP snooping should globally be enabled.
- DHCP snooping should be enabled on the VLAN associated with the entry.
- The port of the entry should not be configured as trusted using the ip dhcp snooping trust command.
- The entry should not be listed as a conflict in the active binding table.
- The entry must contain a valid IP address.
- The entry must contain a valid MAC address.
- The maximum number of entries should not be exceeded.

Example

This example shows how to configure a DHCP snooping entry with IP address 10.1.1.1 and MAC address 00-01-02-03-04-05 at VLAN 2 and port GigabitEthernetv1/0/10 with an expiry time of 100 seconds.

```
GA-MLxxTPoE+# ip dhcp snooping binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface
gi1/0/10 expiry 100
GA-MLxxTPoE+#
```

10.2.8 ip dhcp snooping trust

This command is used to configure a port as a trusted interface for DHCP snooping. Use the **no** form of this command to revert to the default setting.

Syntax

- **ip dhcp snooping trust**
- **no ip dhcp snooping trust**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is available for physical port and port-channel interface configuration.
Ports connected to the DHCP server or to other switches should be configured as trusted interfaces. The ports connected to DHCP clients should be configured as untrusted interfaces. DHCP snooping acts as a firewall between untrusted interfaces and DHCP servers.
When a port is configured as a untrusted interface, the DHCP message arrives at the port on a VLAN that is enabled for DHCP snooping. The Switch forwards the DHCP packet unless any of the following conditions occur (in which case the packet is dropped):

- The Switch port receives a packet (such as a DHCPOFFER, DHCPACK, DHCPNAK, or DHCPLEASEQUERY packet) from a DHCP server outside the firewall.
- If the **ip dhcp snooping verify mac-address** command is enabled, the source MAC in the Ethernet header must be the same as the DHCP client hardware address to pass the validation.
- The untrusted interface receives a DHCP packet that includes a relay agent IP address that is not 0.0.0.0 or the relay agent forward a packet that includes Option 82 to an untrusted interface.
- The router receives a DHCPRELEASE or DHCPDECLINE message from an untrusted host with an entry in the DHCP snooping binding table, and the interface information in the binding table does not match the interface on which the message was received.

In addition to doing the validation, DHCP snooping also create a binding entry based on the IP address assigned to client by the server in DHCP snooping binding database. The binding entry contains information including MAC address, IP address, the VLAN ID and port ID where the client is located, and the expiry of the lease time.

Example

This example shows how to enable DHCP snooping trust for GigabitEthernet1/0/3.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/3
GA-MLxxTPoE+(config-if)# ip dhcp snooping trust
GA-MLxxTPoE+(config-if)#
```

10.2.9 ip dhcp snooping limit entries

This command is used to configure the number of the DHCP snooping binding entries that an interface can learn. Use the **no** form of this command to reset the DHCP message entry limit.

Syntax

- **ip dhcp snooping limit entries** {*NUMBER*}
- **no ip dhcp snooping limit entries**

Parameters

Parameters	Description
NUMBER	Specifies the number of DHCP snooping binding entries limited on a port. The range of value is from 0 to 1024.
no-limit	Specifies no binding entry number limitation.

Default

By default, this option is no-limit.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is available for physical port and port-channel interface configuration. This command only takes effect on untrusted interfaces. The system will stop learning binding entries associated with the port if the maximums number is exceeded.

Example

This example shows how to configure the limit on binding entries allowed on GigabitEthernet1/0/1 to 100.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# ip dhcp snooping limit entries 100
GA-MLxxTPoE+(config-if)#
```

10.2.10ip dhcp snooping limit rate

This command is used to configure the number of the DHCP messages that an interface can receive per second. Use the **no** form of this command to reset the DHCP message rate limiting.

Syntax

- **ip dhcp snooping limit rate** {*VALUE* | **no-limit**}

Parameters

Parameters	Description
VALUE	Specifies the number of DHCP messages that can be processed per second. The valid range is from 1 to 300.
no-limit	Specifies no limitation on the rate.

Default

By default, this option is no-limit.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

When the rate of the DHCP packet exceeds the limitation, the port will be changed to the error disable state.

Example

This example shows how to configure number of DHCP messages that a switch can receive per second on GigabitEthernet1/0/3.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/3
GA-MLxxTPoE+(config-if)# ip dhcp snooping limit rate 100
GA-MLxxTPoE+(config-if)#
```

10.2.11ip dhcp snooping station-move deny

This command is used to disable the DHCP snooping station move state. Use the **no** form of this command to enable the DHCP snooping roaming state.

Syntax

- **ip dhcp snooping station-move deny**
- **no ip dhcp snooping station-move deny**

Parameters

None

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

When DHCP snooping station move is enabled, the dynamic DHCP snooping binding entry with the same VLAN ID and MAC address on the specific port can move to another port if it detects that a new DHCP process belong to the same VLAN ID and MAC address.

Example

This example shows how to disable the roaming state.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip dhcp snooping
GA-MLxxTPoE+(config)# ip dhcp snooping vlan 10
GA-MLxxTPoE+(config)# ip dhcp snooping station-move deny
GA-MLxxTPoE+(config)#
```

10.2.12ip dhcp snooping verify mac-address

This command is used to enable the verification that the source MAC address in a DHCP packet matches the client hardware address. Use the **no** form of this command to disable the verification of the MAC address.

Syntax

- **ip dhcp snooping verify mac-address**
- **no ip dhcp snooping verify mac-address**

Parameters

None

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The DHCP snooping function validates the DHCP packets when they arrive at the port on the VLAN that is enabled for DHCP snooping. By default, DHCP snooping will verify that the source MAC address in the Ethernet header is the same as the DHCP client hardware address to pass the validation.

Example

This example shows how to enable the verification that the source MAC address in a DHCP packet matches the client hardware address.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip dhcp snooping verify mac-address
GA-MLxxTPoE+(config)#
```

10.2.13ip dhcp snooping vlan

This command is used to enable DHCP snooping on a VLAN or a group of VLANs. Use the **no** command to disable DHCP snooping on a VLAN or a group of VLANs.

Syntax

- **ip dhcp snooping vlan** *VLAN-ID* [, | -]
- **no ip dhcp snooping vlan** *VLAN-ID* [, | -]

Parameters

Parameters	Description
VLAN-ID	Specifies the VLAN to enable or disable the DHCP snooping function.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.

Default

By default, DHCP snooping is disabled on all VLANs.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to globally enable DHCP snooping and use the **ip dhcp snooping vlan** command to enable DHCP snooping for a VLAN. The DHCP snooping function snoops the DHCP packets arriving at the untrusted interface on VLAN that is enabled for DHCP snooping. With this function, the DHCP packets come from the untrusted interface can be validated and a DHCP binding database will be constructed for the DHCP snooping enabled VLAN. The binding database provides IP and MAC binding information that can be further used by the IP source guard and dynamic ARP inspection process.

Example

This example shows how to enable DHCP snooping on VLAN 1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip dhcp snooping vlan 10
GA-MLxxTPoE+(config)#
```

This example shows how to enable DHCP snooping on a range of VLANs.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip dhcp snooping vlan 10,15-18
GA-MLxxTPoE+(config)#
```

10.2.14 show ip dhcp snooping

This command is used to display the DHCP snooping configuration.

Syntax

- **show ip dhcp snooping**

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display DHCP snooping configuration settings.

Example

This example shows how to display DHCP snooping configuration settings.

```
GA-MLxxTPoE+# show ip dhcp snooping

DHCP Snooping is enabled
DHCP Snooping is enabled on VLANs:
          10, 15-18
Verification of MAC address is disabled
Station move is permitted.
Information option is not allowed on un-trusted interface

Interface      Trusted   Rate Limit   Entry Limit
-------------- --------- ------------ ------------
Gi1/0/1        no        10           no_limit
Gi1/0/2        no        50           no_limit
Gi1/0/3        yes       no_limit     no_limit

GA-MLxxTPoE+#
```

10.2.15 show ip dhcp snooping binding

This command is used to display DHCP snooping binding entries.

Syntax

- **show ip dhcp snooping binding** [*IP-ADDRESS*] [*MAC-ADDRESS*] [**vlan** *VLAN-ID*] [**interface** [*INTERFACE-ID* [**,** | **-**]]]

Parameters

Parameters	Description
IP-ADDRESS	(Optional) Specifies to display the binding entry based on the IP address.
MAC-ADDRESS	(Optional) Specifies to display the binding entry based on the MAC address.

Parameters	Description
vlan *VLAN-ID*	(Optional) Specifies to display the binding entry based on the VLAN.
interface *INTERFACE-ID*	(Optional) Specifies to display the binding entry based on the port ID.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display DHCP snooping binding entries.

Example

This example shows how to display DHCP snooping binding entries.

```
GA-MLxxTPoE+#show ip dhcp snooping binding

MAC Address       IP Address      Lease(seconds) Type          VLAN Interface
----------------- --------------- -------------- ------------- ---- --------------
00-01-02-03-04-05 10.1.1.10       1500           dhcp-snooping 100  Gi1/0/5
00-01-02-00-00-05 10.1.1.11       1495           dhcp-snooping 100  Gi1/0/5

Total Entries: 2

GA-MLxxTPoE+#
```

This example shows how to display DHCP snooping binding entries by IP 10.1.1.1.

```
GA-MLxxTPoE+# show ip dhcp snooping binding 10.1.1.1

MAC Address       IP Address      Lease (seconds)   Type            VLAN   Interface
----------------- --------------- ----------------  --------------- ------ ----------
00-01-02-03-04-05 10.1.1.1        1500              dhcp-snooping   100    Gi1/0/5

Total Entries: 1

GA-MLxxTPoE+#
```

This example shows how to display DHCP snooping binding entries by IP 10.1.1.11 and MAC 00-01-02-00-00-05.

```
GA-MLxxTPoE+# show ip dhcp snooping binding 10.1.1.11 00-01-02-00-00-05

MAC Address       IP Address      Lease(seconds) Type           VLAN Interface
----------------- --------------- -------------- -------------- ---- --------------
00-01-02-00-00-05 10.1.1.11       1495           dhcp-snooping  100  Gi1/0/5

Total Entries: 1

GA-MLxxTPoE+#
```

This example shows how to display DHCP snooping binding entries by IP 10.1.1.1 and MAC 00-01-02-03-04-05 on VLAN 100.

```
GA-MLxxTPoE+# show ip dhcp snooping binding 10.1.1.11 00-01-02-00-00-05 vlan 100

MAC Address       IP Address      Lease(seconds) Type           VLAN Interface
----------------- --------------- -------------- -------------- ---- --------------
00-01-02-03-04-05 10.1.1.1        1500           dhcp-snooping  100  Gi1/0/5

Total Entries: 1

GA-MLxxTPoE+#
```

This example shows how to display DHCP snooping binding entries by VLAN 100.

```
GA-MLxxTPoE+# show ip dhcp snooping binding vlan 100

MAC Address       IP Address      Lease(seconds) Type           VLAN Interface
----------------- --------------- -------------- -------------- ---- --------------
00-01-02-03-04-05 10.1.1.10       1500           dhcp-snooping  100  Gi1/0/5
00-01-02-00-00-05 10.1.1.11       1495           dhcp-snooping  100  Gi1/0/5

Total Entries: 2

GA-MLxxTPoE+#
```

This example shows how to display DHCP snooping binding entries by gi1/0/5.

```
GA-MLxxTPoE+# show ip dhcp snooping binding interface gi1/0/5

MAC Address       IP Address      Lease(seconds) Type           VLAN Interface
----------------- --------------- -------------- -------------- ---- --------------
00-01-02-03-04-05 10.1.1.10       1500           dhcp-snooping  100  Gi1/0/5
00-01-02-00-00-05 10.1.1.11       495            dhcp-snooping  100  Gi1/0/5

Total Entries: 2

GA-MLxxTPoE+#
```

Display Parameters

Parameters	Description
MAC Address	The client hardware MAC address.
IP Address	The client IP address assigned from the DHCP server.
Lease (seconds)	The IP address lease time.
Type	The Binding type configured from the CLI or dynamically learned.
VLAN	The VLAN ID.
Interface	The interface that connects to the DHCP client host.

10.2.16show ip dhcp snooping database

This command is used to display the statistics of the DHCP snooping database.

Syntax

- show ip dhcp snooping database

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display DHCP snooping database statistics.

Example

This example shows how to display DHCP snooping database statistics.

```
GA-MLxxTPoE+#show ip dhcp snooping database

URL:  tftp:  //10.0.0.2/store/dhcp-snp-bind
Write Delay Time:  300 seconds

Last ignored bindings counters:
Binding collisions :   0         Expired    lease  :   0
Invalid interfaces :   0         Unsupported vlans :   0
Parse failures     :   0         Checksum errors   :   0

GA-MLxxTPoE+#
```

Display Parameters

Parameters	Description
Binding Collisions	The number of entries that created collisions with exiting entries in DHCP snooping database.
Expired leases	The number of entries that expired in the DHCP snooping database.
Invalid interfaces	The number of interfaces that received the DHCP message but DHCP snooping is not performed.
Parse failures	The number of illegal DHCP packets.
Checksum errors	The number of calculated checksum values that is not equal to the stored checksum.
Unsupported vlans	The number of the entries of which the VLAN is disabled.

10.3 IP Source Guard Commands

10.3.1 ip verify source vlan dhcp-snooping

This command is used to enable IP source guard for a port. Use the **no** form of this command to disable IP source guard.

Syntax

- **ip verify source vlan dhcp-snooping [ip-mac]**
- **no ip verify source vlan dhcp-snooping [ip-mac]**

Parameters

Parameters	Description
ip-mac	(Optional) Specifies to check both IP address and MAC address of the received IP packets.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command is available for physical port and port channel configuration. Use this command to enable the IP source guard on the configured port.
When a port is enabled for IP source guard, the IP packet that arrives at the port will be validated via the port ACL. Port ACL is a hardware mechanism and its entry can come from either a manual configured entry or the DHCP snooping binding database. The packet that fails to pass the validation will be dropped. There are two types of validations.

- If **ip-mac** is not specified, the validation is based on the source IP address and VLAN check only.
- If **ip-mac** is specified, the validation is based on the source MAC address, VLAN and IP address.

Example

This example shows how to enable IP Source Guard for GigabitEthernet1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# ip verify source vlan dhcp-snooping
GA-MLxxTPoE+(config-if)#
```

10.3.2 ip source binding

This command is used to create a static entry used for IP source guard. Use the **no** form of this command to delete a static binding entry.

Syntax

- **ip source binding** *MAC-ADDRESS* **vlan** *VLAN-ID IP-ADDRESS* **interface** *INTERFACE-ID* [**,** | **-**]
- **no ip source binding** *MAC-ADDRESS* **vlan** *VLAN-ID IP-ADDRESS* **interface** *INTERFACE-ID* [**,** | **-**]

Parameters

Parameters	Description
MAC-ADDRESS	Specifies the MAC address of the IP-to-MAC address binding entry.
vlan *VLAN-ID*	Specifies the VLAN that the valid host belongs to.
IP-ADDRESS	Specifies the IP address of the IP-to-MAC address binding entry.
interface *INTERFACE-ID*	Specifies the port that the valid host is connected.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to create a static binding entry used for IP source guard checking. Use the **no** command to delete a static binding entry. The parameters specified for the command must exactly match the configured parameters to be deleted.
If the MAC address and the VLAN for the configured entry already exist, the existing binding entry is updated. The interface specified for the command can be a physical port or a port-channel interface.

Example

This example shows how to configure an IP Source Guard entry with the IP address 10.1.1.1 and MAC address 00-01-02-03-04-05 at VLAN 2 on GigabitEthernet1/0/10.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface gi1/0/10
GA-MLxxTPoE+(config)#
```

This example shows how to delete an IP Source Guard entry with the IP address 10.1.1.1 and MAC address 00-01-02-03-04-05 at VLAN 2 on GigabitEthernet1/0/10.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# no ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface gi1/0/10
GA-MLxxTPoE+(config)#
```

10.3.3 show ip source binding

This command is used to display an IP-source guard binding entry.

Syntax

- **show ip source binding** [*IP-ADDRESS*] [*MAC-ADDRESS*] [**dhcp-snooping** | **static**] [**vlan** *VLAN-ID*] [**interface** *INTERFACE-ID* [**,** | **-**]]

Parameters

Parameters	Description
IP-ADDRESS	(Optional) Specifies to display the IP-source guard binding entry based on IP address.
MAC-ADDRESS	(Optional) Specifies to display the IP-source guard binding entry based on MAC address.
dhcp-snooping	(Optional) Specifies to display the IP-source guard binding entry learned by DHCP binding snooping.
static	(Optional) Specifies to display the IP-source guard binding entry that is manually configured.
vlan *VLAN-ID*	(Optional) Specifies to display the IP-source guard binding entry based on VLAN.
interface *INTERFACE-ID*	(Optional) Specifies to display the IP-source guard binding entry based on ports.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

IP source guard binding entries are either manually configured or automatically learned by DHCP snooping to guard IP traffic.

Example

This example shows how to display IP Source Guard binding entries without any parameters.

```
GA-MLxxTPoE+#show ip source binding

MAC Address       IP Address      Lease(sec)  Type          VLAN Interface
----------------- --------------- ---------- ------------- ---- ---------
00-01-01-01-01-01 10.1.1.10        infinite  static        100  Gi1/0/3
00-01-01-01-01-10 10.1.1.11          3120    dhcp-snooping 100  Gi1/0/3

Total Entries: 2

GA-MLxxTPoE+#
```

This example shows how to display IP Source Guard binding entries by IP address 10.1.1.10.

```
GA-MLxxTPoE+# show ip source binding 10.1.1.10

MAC Address       IP Address      Lease(sec)  Type          VLAN   Interface
----------------- --------------- ---------- ------------- ----- ----------
00-01-01-01-01-01 10.1.1.10        infinite  static        100    Gi1/0/3

Total Entries: 1

GA-MLxxTPoE+#
```

This example shows how to display IP Source Guard binding entries by IP address 10.1.1.11, MAC address 00-01-01-01-01-10, at VLAN 100 on GigabitEthernet1/0/3 and learning by DHCP snooping.

```
GA-MLxxTPoE+# show ip source binding 10.1.1.10 00-01-01-01-01-10 dhcp-snooping vlan
100 interface Gi1/0/3

MAC Address       IP Address      Lease(sec)  Type          VLAN   Interface
----------------- --------------- ---------- ------------- ----- -----------
00-01-01-01-01-10 10.1.1.11          3564    dhcp-snooping 100    Gi1/0/3

Total Entries: 1

GA-MLxxTPoE+#
```

Display Parameters

Parameters	Description
MAC Address	The client's hardware MAC address.
IP Address	The client's IP address assigned from the DHCP server or configured by the user.
Lease (sec)	The IP address lease time.
Type	The binding type. Static bindings are configured manually. Dynamic binding are learned from DHCP snooping.
VLAN	The VLAN number of the client interface.

Parameters	Description
Interface	The interface that connects to the DHCP client host.

10.3.4 show ip verify source

This command is used to display the hardware port ACL entry on a particular interface.

Syntax

- **show ip verify source [interface** *INTERFACE-ID* **[, | -]]**

Parameters

Parameters	Description
interface *INTERFACE-ID*	(Optional) Specifies a port or a range of ports to configure.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display the hardware port ACL entries for a port in the hardware table. It indicates the hardware filter behavior that IP source guard is verified upon.

Example

This example shows how to display when DHCP snooping is enabled on VLANs 100 to 110, the interface with IP source filter mode that is configured as IP, and that there is an existing IP address binding 10.1.1.1 on VLAN 100.

```
GA-MLxxTPoE+#show ip verify source interface gi1/0/3

Interface       Filter-type Filter-mode IP address      MAC address       VLAN
---------       ----------- ----------- --------------- ----------------- ----
Gi1/0/3         ip          active      10.1.1.1              -           100
Gi1/0/3         ip          active      deny-all              -           101-120

Total Entries: 2

GA-MLxxTPoE+#
```

This example shows how to display when the interface has an IP source filter mode that is configured as IP MAC and an existing IP MAC that binds IP address 10.1.1.10 to MAC address 00-01-01-01-01-01 on VLAN 100 and IP address 10.1.1.11 to MAC address 00-01-01-01-01-10 on VLAN 101.

```
GA-MLxxTPoE+# show ip verify source interface Gi1/0/3

Interface       Filter-type Filter-mode IP address      MAC address       VLAN
---------       ----------- ----------- --------------- ----------------- ----
Gi1/0/3         ip-mac      active      10.1.1.10       00-01-01-01-01-01 100
Gi1/0/3         ip-mac      active      10.1.1.11       00-01-01-01-01-10 101
Gi1/0/3         ip-mac      active      deny-all              -           102-120

Total Entries: 3

GA-MLxxTPoE+#
```

Display Parameters

Parameters	Description
Interface	The interface that has IP inspection enabled.
Filter-type	The type of IP Source Guard in operation. **ip:** Only use an IP address to authorize IP packets. **ip-mac:** Use the IP and MAC address to authorize IP packets.
Filter-Mode	**active:** Actively verify IP source entries. **inactive-trust-port:** Enable DHCP snooping to trust ports with no IP source entry verification active. **inactive-no-snooping-vlan:** No DHCP snooping VLAN configured with no IP source entry verification active.
IP address	The client's IP address assigned from the DHCP server or configured by the user.
MAC address	The client's MAC address.
VLAN	The VLAN number of the client interface.

10.4 DHCPv6 Client Commands

10.4.1 clear ipv6 dhcp client

This command is used to restart the DHCPv6 client on an interface.

Syntax

- **clear ipv6 dhcp client** *INTERFACE-ID*

Parameters

Parameters	Description
INTERFACE-ID	Specifies the VLAN interface to restart the DHCPv6 client.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

This command restarts the IPv6 DHCP client on the specified interface.

Example

This example shows how to restart the DHCPv6 client for interface VLAN 1.

```
GA-MLxxTPoE+# clear ipv6 dhcp client vlan1
GA-MLxxTPoE+#
```

10.4.2 ipv6 dhcp client pd

This command is used to enable the Dynamic Host Configuration Protocol (DHCP) IPv6 client process to request the prefix delegation through a specified interface. Use the **no** form of this command to disable the request.

Syntax

- **ipv6 dhcp client pd** {*PREFIX-NAME* | **hint** *IPV6-PREFIX*} [**rapid-commit**]
- **no ipv6 dhcp client pd**

Parameters

Parameters	Description
PREFIX-NAME	Specifies the IPv6 general prefix name with a maximum of 12 characters.
hint *IPV6-PREFIX*	Specifies the IPv6 prefix to be sent in the message as a hint.
rapid-commit	Specifies to use a two-message exchange instead of the standard four-message exchange between the Requesting Router (RR) and the Delegating Router (DR) to obtain the network configuration settings from the DHCPv6 Server.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to enable the prefix delegation request through an interface. The interface being configured will be in DHCP client mode. The prefix acquired from the server will be stored in the IPv6 general prefix pool represented by the general prefix name of the command, which will be in turn used in configuration of IPv6 addresses. Only one general prefix name can be specified for DHCPv6 PD on an interface. However, a general prefix name can be specified for DHCPv6 PD on multiple interfaces.

The standard four-message exchange between the DR and the RR includes four messages: *SOLICIT*, *ADVERTISE*, *REQUEST*, and *REPLY*. When the **rapid-commit** parameter is specified, the RR will notify the DR in the *SOLICIT* message that it can skip receiving the *ADVERTISE* message and sending *REQUEST* message, and proceed directly with receiving the *REPLY* message from DR to complete a two-message exchange instead of the standard four-message exchange. The *REPLY* message contains the network configuration settings.
The **rapid-commit** parameter must be enabled on both the DR and the RR to function properly.
If the **hint** parameter is specified for the command, the specified hint prefix will be included in the transmitted solicit or request message as a hint to the prefix delegation server. Only one hint prefix can be configured.
When the client receives advertisement from multiple servers, the client will take the server with best preference value. The client can accept multiple prefixes delegated from a server.
The DHCP for IPv6 client, server and relay functions are mutually exclusive on an interface.

Example

This example shows how to configure an IPv6 address based on the general prefix "dhcp-prefix" on VLAN 2 and enables DHCPv6 prefix delegation on VLAN 1 with "dhcp-prefix" as the general prefix name and with the rapid commit option.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface vlan2
GA-MLxxTPoE+(config-if)# ipv6 address dhcp-prefix 0:0:0:7272::72/64
GA-MLxxTPoE+(config-if)# exit
GA-MLxxTPoE+(config)# interface vlan1
GA-MLxxTPoE+(config-if)# ipv6 dhcp client pd dhcp-prefix rapid-commit
GA-MLxxTPoE+(config-if)#
```

10.4.3 show ipv6 dhcp

This command is used to display the DHCPv6 related settings on the interface.

Syntax

- **show ipv6 dhcp [interface [***INTERFACE-ID***]]**

Parameters

Parameters	Description
INTERFACE-ID	Specifies the VLAN interface to display the DHCPv6 related settings.

Default

None.

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display the device's DHCPv6 DUID or use the **show ipv6 dhcp interface** command to display DHCPv6 related setting for interfaces. If the interface ID is not specified, all interfaces with the DHCPv6 function will be displayed.

Example

This example shows how to display the DHCPv6 DUID for the device.

```
GA-MLxxTPoE+# show ipv6 dhcp

This device's DUID is 0001000111A8040D001FC6D1D47B.

GA-MLxxTPoE+#
```

This example shows how to display the DHCPv6 setting for interface VLAN 1, when VLAN 1 is DHCPv6 disabled.

```
GA-MLxxTPoE+# show ipv6 dhcp interface vlan1

vlan1 is not in DHCPv6 mode.

GA-MLxxTPoE+#
```

This example shows how to display the DHCPv6 setting for all VLANs. Only VLANs that are DHCPv6 enabled are displayed.

```
GA-MLxxTPoE+# show ipv6 dhcp interface

vlan1 is in client mode
  State is OPEN
  List of known servers:
    Reachable via address: FE80::200:11FF:FE22:3344
    Configuration parameters:
        IA PD: IA ID 1, T1 40, T2 64
          Prefix: 2000::/48
                preferred lifetime 80, valid lifetime 100
  Prefix name: yy
  Rapid-Commit: disabled

GA-MLxxTPoE+#
```

10.5 DNS (Domain Name System) Commands

10.5.1 clear host

This command is used to clear the dynamically learned host entries in the privileged user mode.

Syntax

- **clear host** {**all** | [*HOST-NAME*]}

Parameters

Parameters	Description
all	Specifies to clear all host entries.
HOST-NAME	(Optional) Specifies to delete the specified dynamically learned host entry.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to delete a host entry or all host entries which are dynamically learned by the DNS resolver or caching server.

Example

This example shows how to delete the dynamically entry “www.abc.com” from the host table.

```
GA-MLxxTPoE+# clear host www.abc.com
GA-MLxxTPoE+#
```

10.5.2 ip dns server

This command is used to enable the DNS caching name server function. Use the **no** form of this command to disable the DNS caching name server function.

Syntax

- **ip dns server**
- **no ip dns server**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The system supports the DNS caching name server function. When the caching name server function is enabled and IP domain-lookup, the system forwards the DNS query packet to the configured name server. The answer replied by the name server will be cached and used to answer the subsequent queries.

Example

This example shows how to enable the DNS caching name server function.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip dns server
GA-MLxxTPoE+(config)#
```

10.5.3 ip dns lookup

This command is used to enable DNS searching dynamic cached or static created host entries. Use the **no** form of this command to disable DNS searching dynamic or static host entries.

Syntax

- **ip dns lookup [static] [cache]**
- **no ip dns lookup [static] [cache]**

Parameters

Parameters	Description
static	(Optional) Specifies to enable or disable the lookup of static entries before asking the name server.
cache	(Optional) Specifies to enable or disable the lookup of the dynamic cache before asking the name server.

Default

Enable lookup static and cache.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

When the system tries to lookup a domain name, by default, it will look in the static and dynamic cache first and then send a query to the name server if no matching entries were found. Use this command to disable the lookup option of static or dynamic cache entries before sending requests to the name server. If this command is used without options, then the static and cache options are enabled or disabled at the same time.

Example

This example shows how to enable the lookup of a static host for answering the request.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip dns lookup static
GA-MLxxTPoE+(config)#
```

10.5.4 ip domain lookup

This command is used to enable the DNS to carry out the domain name resolution. Use the **no** form of this command to disable the DNS domain name resolution function.

Syntax

- **ip domain lookup**
- **no ip domain lookup**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use the **ip domain lookup** command to enable the domain name resolution function. The DNS resolver sends the query to the configured name server. The answer replied by the name server will be cached for answering the subsequent requests.

Example

This example shows how to enable the DNS domain name resolution function.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip domain lookup
GA-MLxxTPoE+(config)#
```

10.5.5 ip host

This command is used to configure the static mapping entry for the host name and the IP address in the host table. Use the **no** form of this command to remove the static host entry.

Syntax

- **ip host** *HOST-NAME* {*IP-ADDRESS* | *IPV6-ADDRESS*}
- **no ip host** *HOST-NAME* {*IP-ADDRESS* | *IPV6-ADDRESS*}

Parameters

Parameters	Description
HOST-NAME	Specifies the host name of the equipment.
IP-ADDRESS	Specifies the IPv4 address of the equipment.
IPV6-ADDRESS	Specifies the IPv6 address of the equipment.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The host name specified in this command needs to be qualified. To delete a static host entry, use the **no** command.

Example

This example shows how to configure the mapping of the host name "www.abc.com" and the IP address 192.168.5.243.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip host www.abc.com 192.168.5.243
GA-MLxxTPoE+(config)#
```

10.5.6 ip name-server

This command is used to configure the IP address of a domain name server. Use the **no** form of this command to delete the configured domain name server.

Syntax

- **ip name-server** {*IP-ADDRESS* | *IPV6-ADDRESS*} [{*IP-ADDRESS2* | *IPV6-ADDRESS2*}]
- **no ip name-server** {*IP-ADDRESS* | *IPV6-ADDRESS*} [{*IP-ADDRESS2* | *IPV6-ADDRESS2*}]

Parameters

Parameters	Description
IP-ADDRESS	Specifies the IPv4 address of the domain name server.
IPV6-ADDRESS	Specifies the IPv6 address of the domain name server.
IP-ADDRESS2	Specifies multiple IP addresses, separated by spaces. Up to two servers can be specified.
IPV6-ADDRESS2	Specifies multiple IPv6 addresses, separated by spaces. Up to two servers can be specified.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to configure a DNS server. When the system cannot obtain an answer from a DNS server, it will attempt the subsequent server until it receives a response. If name servers are already configured, the servers configured later will be added to the server list. The user can configure up to 4 name servers.

Example

This example shows how to configure the domain name server 192.168.5.134 and 5001:5::2.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip name-server 192.168.5.134 5001:5::2
GA-MLxxTPoE+(config)#
```

10.5.7 ip name-server timeout

This command is used to configure the timeout value for the name server. Use the **no** form of this command to revert to the default setting.

Syntax

- **ip name-server timeout** *SECONDS*
- **no ip name-server timeout**

Parameters

Parameters	Description
SECONDS	Specifies the maximum time to wait for a response from a specified name server. This value must be between 1 and 60.

Default

By default, this value is 3 seconds.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to configure the DNS maximum time value to wait for a response from a specified name server.

Example

This example shows how to configure the timeout value to 5 seconds.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ip name-server timeout 5
GA-MLxxTPoE+(config)#
```

10.5.8 show hosts

This command is used to display the DNS configuration.

Syntax

- show hosts

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display DNS related configuration information.

Example

This example shows how to display DNS related configuration information.

```
GA-MLxxTPoE+#show hosts

 Number of Static Entries:   1
 Number of Dynamic Entries:  0

 Host Name:          www.abc.com
 IP Address:         192.168.5.243
 TTL:                forever


GA-MLxxTPoE+#
```

10.5.9 show ip name-server

This command is used to display the current DNS name servers.

Syntax

- show ip name-server

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display the DNS name servers.

Example

This example shows how to display the DNS name servers.

```
GA-MLxxTPoE+#show ip name-server

 Static name server:
 192.168.5.134
 5001:5::2

 Dynamic name server:

GA-MLxxTPoE+#
```

11 Authentication Function

11.1 Authentication, Authorization, and Accounting (AAA) Commands

11.1.1 aaa new-model

This command is used to enable AAA for the authentication or accounting function. Use the **no** form of this command to disable the AAA function.

Syntax

- **aaa new-model**
- **no aaa new-model**

Parameters

None

Default

By default, this feature is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

The user should use the **aaa new-model** command to enable AAA before the authentication and accounting via the AAA method lists take effect. If AAA is disabled, the login user will be authenticated via the local user account table created by the **username** command. The enable password will be authenticated via the local table which is defined via the **enable password** command.

Example

This example shows how to enable the AAA function.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)# aaa new-model
GA-MLxxTPoE+(config)#
```

11.1.2 aaa accounting commands

This command is used to configure the accounting method list used for all commands at the specified privilege level. Use the **no** form of this command to remove an accounting method list.

Syntax

- **aaa accounting commands** *LEVEL* {**default** | *LIST-NAME*} {**start-stop** *METHOD1* [*METHOD2*...] | **none**}
- **no aaa accounting commands** *LEVEL* {**default** | *LIST-NAME*}

Parameters

Parameters	Description
LEVEL	Specifies to do accounting for all configure commands at the specified privilege level. The privilege level is between 1 and 15.
default	Specifies to configure the default method list for accounting.
LIST-NAME	Specifies the name of the method list. This name can be up to 32 characters long.
METHOD1 [*METHOD2*...]	Specifies the list of methods that the accounting algorithm tries in the given sequence. Enter at least one method or enter up to four methods. The following are keywords that can be used to specify a method. **group tacacs+** - Specifies to use the servers defined by the **tacacs-server host** command. **group** *GROUP-NAME* - Specifies to use the server groups defined by the **aaa group server tacacs+** command.
none	Specifies not to perform accounting.

Default

No AAA accounting method is configured.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to configure the method list for accounting of commands.

Example

This example shows how to create a method list for accounting of the privilege level of 15 using TACACS+ and sends the accounting messages at the start and end time of access.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)# aaa accounting commands 15 list-1 start-stop group tacacs+
GA-MLxxTPoE+(config)#
```

11.1.3 aaa accounting exec

This command is used to configure the method list used for EXEC accounting for a specific line. Use the **no** form of this command to delete an Exec accounting method list.

Syntax

- **aaa accounting exec {default |** *LIST-NAME*} {**start-stop** *METHOD1* [*METHOD2*...] **| none}**
- **no aaa accounting exec {default |** *LIST-NAME*}

Parameters

Parameters	Description
default	Specifies to configure the default method list for EXEC accounting.
LIST-NAME	Specifies the name of the method list. This name can be up to 32 characters long.

Parameters	Description
METHOD1 [METHOD2...]	Specifies the list of methods that the accounting algorithm tries in the given sequence. Enter at least one method or enter up to four methods. The following are keywords that can be used to specify a method. **group radius** - Specifies to use the servers defined by the **radius-server host** command. **group tacacs+** - Specifies to use the servers defined by the **tacacs-server host** command. **group** *GROUP-NAME* - Specifies to use the server groups defined by the **aaa group server radius** and **aaa group server tacacs+** commands.
none	Specifies not to perform accounting.

Default

No AAA accounting method is configured.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to configure the method list for EXEC accounting.

Example

This example shows how to create a method list for accounting of user activities using RADIUS, which will send accounting messages at the start and end time of access.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)# aaa accounting exec list-1 start-stop group radius
GA-MLxxTPoE+(config)#
```

11.1.4 aaa accounting network

This command is used to account user activity in accessing the network. Use the **no** form of this command to remove the accounting method list.

Syntax

- **aaa accounting network default {start-stop** *METHOD1* **[***METHOD2***...] | none}**
- **no aaa accounting network default**

Parameters

Parameters	Description
network	Specifies to perform accounting of network related service requests.
start-stop	Specifies to send accounting messages at both the start time and the end time of access. Users are allowed of access the network regardless of whether the start accounting message enables the accounting successfully.
default	Specifies to configure the default method list for network accounting.
METHOD1 **[***METHOD2***...]**	Specifies the list of methods that the accounting algorithm tries in the given sequence. Enter at least one method or enter up to four methods. The following are keywords that can be used to specify a method. **group radius** - Specifies to use the servers defined by the **radius-server host** command. **group tacacs+** - Specifies to use the servers defined by the **tacacs-server host** command. **group** *GROUP-NAME* - Specifies to use the server groups defined by the **aaa group server radius** and **aaa group server tacacs+** commands.
none	Specifies not to perform accounting.

Default

No AAA accounting method is configured.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to configure the accounting method list for network access fees. For the default method list to take effect, enable AAA first by using the **aaa new-model** command. The accounting system is disabled if the default method list is not configured.

Example

This example shows how to enable accounting of the network access fees using RADIUS and sends the accounting messages at the start and end time of access:

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)# aaa accounting network default start-stop group radius
GA-MLxxTPoE+(config)#
```

11.1.5 aaa accounting system

This command is used to account system events. Use the **no** form of this command to remove the accounting method list.

Syntax

- **aaa accounting system default** {**start-stop** *METHOD1* [*METHOD2*...] | **none**}
- **no aaa accounting system default**

Parameters

Parameters	Description
system	Specifies to perform accounting for system-level events.
start-stop	Specifies to send accounting messages at both the start time and the end time of access. Users are allowed to access the network regardless of whether the start accounting message enables the accounting successfully.
default	Specifies to configure the default method list for system accounting.

Parameters	Description
METHOD1 [*METHOD2*...]	Specifies the list of methods that the accounting algorithm tries in the given sequence. Enter at least one method or enter up to four methods. The following are keywords that can be used to specify a method. **group radius** - Specifies to use the servers defined by the **radius-server host** command. **group tacacs+** - Specifies to use the servers defined by the **tacacs-server host** command. **group** *GROUP-NAME* - Specifies to use the server groups defined by the **aaa group server radius** and **aaa group server tacacs+** commands.
none	Specifies not to perform accounting.

Default

No AAA accounting method is configured.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to configure the accounting method list for system-events such as reboot, reset events. For the default method list to take effect, enable AAA first by using the **aaa new-model** command. The accounting system is disabled if the default method list is not configured.

Example

This example shows how to enable accounting of the system events using RADIUS and sends the accounting messages while system event occurs:

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)# aaa accounting system default start-stop group radius
GA-MLxxTPoE+(config)#
```

11.1.6 aaa authentication auth-mac

This command is used to configure the authentication local user account for MAC authentication. Use the **no** form of this command to remove the specific user.

Syntax

- **aaa authentication auth-mac** *MAC-ADDRESS* **vlan** *VLAN-ID* [**filter-id** *NUMBER*] **step-auth** {**no** | **dot1x** | **web** | **any**}
- **no aaa authentication auth-mac** *MAC-ADDRESS*

Parameters

Parameters	Description
auth-mac *MAC-ADDRESS*	Specifes the MAC address for the MAC-authentication local account.
vlan *VLAN-ID*	Specifes the target VLAN of the authentication account.
filter-id *NUMBER*	Specifes the ACL number.
step-auth	Specifies the next authentication method for 2-step authentication. **no** - Specifies to use no next authentication method. **dot1x** - Specifies to use 802.1X authentication as the next authentication method. **web** - Specifies to use web authentication as the next authentication method. **any** - Specifies to use 802.1X and web authentication as the next authentication method.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

This command is used to configure the local account and the next authentication method for MAC authentication.

Example

This example shows how to set MAC 00-01-02-03-04-05 for MAC authentication.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)# aaa authentication auth-mac 00-01-02-03-04-05 vlan 100 filter-id 3999 step-auth any
GA-MLxxTPoE+(config)#
```

11.1.7 aaa authentication auth-user

This command is used to configure the local user account for authentication. Use the **no** form of this command to remove the specific user.

Syntax

- **aaa authentication auth-user** *STRING* {**password** *STRING* [**encrypt**] | **encrypt-password** *STRING*} **vlan** *VLAN-ID* [**filter-id** *NUMBER*] **auth-type** {**both** | **web** | **dot1x**} **step-auth** {**enable** | **disable**}
- **no aaa authentication auth-user** *STRING*

Parameters

Parameters	Description
auth-user *STRING*	Specifes the username of the authentication account. The maximum length is 32 characters.
password *STRING*	Specifies the password of the authentication account in clear text form. The password can between 1 and 32 clear text characters.
encrypt	(Optional) Specifies to enable the password encryption for the authentication account. The password will be saved in the encrypted format.
encrypt-password *STRING*	Specifies the password in the encrypted format. The password can between 1 and 56 clear text characters.
vlan *VLAN-ID*	Specifes the target VLAN of the authentication account.
filter-id *NUMBER*	Specifes the ACL number.
auth-type	Specifes the authentication method. **both** - Specifes to use both 802.1X and web authentication. **dot1x** - Specifes to use 802.1X authentication. **web** - Specifes to use web authentication.

Parameters	Description
step-auth	Specifies the next authentication method for 2-step authentication. **enable** - Specifies to enable the next authentication method for 802.1X authentication. **disable** - Specifies to remove the next authentication method for 802.1X authentication.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to configure the local user account for authentication. The **step-auth** parameter is used to specify the next authentication method for 802.1X authentication. If the authentication is configured as web authentication, the **step-auth** parameter will be ignored.

Example

This example shows how to configure the local user account for 802.1X authentication.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)# aaa authentication auth-user user password 123 encrypt vlan 10
filter-id 3999 auth-type dot1x step-auth enable
GA-MLxxTPoE+(config)#
```

11.1.8 aaa authentication enable

This command is used to configure the default method list used for determining access to the privileged EXEC level. Use the **no** form of this command to remove the default method list.

Syntax

- **aaa authentication enable default** *METHOD1* [*METHOD2*...]

- no aaa authentication enable default

Parameters

Parameters	Description
METHOD1 [*METHOD2*...]	Specifies the list of methods that the authentication algorithm tries in the given sequence. Enter at least one method or enter up to four methods. The following are keywords that can be used to specify a method. **enable** - Specifies to use the local enable password for authentication. **group radius** - Specifies to use the servers defined by the **radius-server host** command. **group tacacs+** - Specifies to use the servers defined by the **tacacs-server host** command. **group** *GROUP-NAME* - Specifies to use the server groups defined by the **aaa group server radius** and **aaa group server tacacs+** commands. **none** - Normally, the method is listed as the last method. The user will pass the authentication if it is not denied by the previous authentication method.

Default

No AAA authentication method is configured.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to configure the default authentication method list for determining access to the privileged EXEC level when the **enable [privilege** *LEVEL*] command is entered. The authentication with the RADIUS server will be based on the privilege level and take either “enable12” or “enable15” as the user name.

Example

This example shows how to set the default method list for authenticating. The method tries the server group “group2”.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)# aaa authentication enable default group group2
GA-MLxxTPoE+(config)#
```

11.1.9 aaa authentication dot1x

This command is used to configure the primary and secondary database for 802.1X authentication. Use the **no** form of this command to revert to the default setting.

Syntax

- **aaa authentication dot1x {primary radius secondary {local | none} | primary local secondary none}**
- **no aaa authentication dot1x**

Parameters

Parameters	Description
primary radius secondary none	We will use only the RADIUS server. If communication with the RADIUS server fails, it will be treated as authentication approval, and communication will be allowed.
primary radius secondary local	The RADIUS server will be used first. In the case of authentication denial by the RADIUS server, or if communication with the RADIUS server fails, the local database will be used.
primary local secondary none	Only the local database will be used.

Default

The primary database uses the local database, and the secondary database is not used.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to configure the primary and secondary database for 802.1X authentication.

Example

This example shows how to set the primary database to use the RADIUS server and the secondary database to the local database for 802.1X authentication.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)# aaa authentication dot1x primary radius secondary local
GA-MLxxTPoE+(config)#
```

11.1.10 aaa authentication login

This command is used to configure the method list used for login authentication Use the **no** form of this command to remove a login method list.

Syntax

- **aaa authentication login** {**default** | *LIST-NAME*} *METHOD1* [*METHOD2*...]
- **no aaa authentication login** {**default** | *LIST-NAME*}

Parameters

Parameters	Description
default	Specifies to configure the default method list for login authentication.
LIST-NAME	Specifies the name of the method list other than the default method list. This name can be up to 32 characters long.

Parameters	Description
METHOD1 [*METHOD2*...]	Specifies the list of methods that the authentication algorithm tries in the given sequence. Enter at least one method or enter up to four methods. The following are keywords that can be used to specify a method. **local** - Specifies to use the local database for authentication. **group radius** - Specifies to use the servers defined by the **radius-server host** command. **group tacacs+** - Specifies to use the servers defined by the **tacacs-server host** command. **group** *GROUP-NAME* - Specifies to use the server groups defined by the **aaa group server radius** and **aaa group server tacacs+** commands. **none** - Normally, the method is listed as the last method. The user will pass authentication if it is not denied by the previous authentication method.

Default

No AAA authentication method list is configured.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to configure the authentication method list used for login authentication. Multiple method lists can be configured. The default keyword is used to define the default method list.
If authentication uses the default method list but the default method list does not exist, then the authentication will be performed via the local database.
The login authentication authenticates the login user name and password, and also assigns the privilege level to the user based on the database.
A method list is a sequential list describing the authentication methods to be queried in order to authenticate a user. Method lists enable you to designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The switch system uses

the first listed method to authenticate users. If that method fails to respond, the switch system selects the next authentication method listed in the method list. This process continues until there is successful communication with a listed authentication method or all methods defined in the method list are exhausted. It is important to note that the switch system attempts authentication with the next listed authentication method only when there is no response from the previous method. If authentication fails at any point in this cycle, meaning that the security server or local username database responds by denying the user access, the authentication process stops and no other authentication methods are attempted.

Example

This example shows how to set the default login methods list for authenticating of login attempts.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)# aaa authentication login default group group2 local
GA-MLxxTPoE+(config)#
```

11.1.11aaa authentication mac

This command is used to configure the primary and secondary database, or auth-fail-action for MAC authentication. Use the **no** form of this command to revert to the default setting.

Syntax

- **aaa authentication mac {primary radius secondary {local | none} | primary local secondary {radius | none}}**
- **aaa authentication mac auth-fail-action {secondary-db | stop}**
- **no aaa authentication mac**

Parameters

Parameters	Parameters auth-fail-action	Description
primary local secondary none (Default)	**secondary-db (Default)**	The authentication function will not operate. It will be treated as authentication approval, and communication will be allowed.
primary local secondary none or primary local secondary radius	**stop**	Only the local database will be used. If there is a denial in the local database, communication will be prohibited.

Parameters	Parameters auth-fail-action	Description
primary radius secondary none	**stop**	Only the RADIUS server will be used. If there is a denial on the RADIUS server, communication will be prohibited. If communication with the RADIUS server fails, it will be treated as authentication approval.
primary radius secondary local	**stop**	The RADIUS server will be used first. If there is a denial on the RADIUS server, communication will be prohibited. If communication with the RADIUS server fails, the local database will be used.
primary radius secondary local	**secondary-db**	The RADIUS server will be used first. If there is a denial on the RADIUS server, or if communication with the RADIUS server fails, the local database will be used.
primary local secondary radius	**secondary-db**	The local database will be used first. If there is a denial in the local database, the RADIUS server will be used.

Default

The authentication function will not operate.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to configure the primary and secondary database, or auth-fail-action for MAC authentication.

Example

This example shows how to set the primary database to use the RADIUS server and the secondary database to the local database for MAC authentication.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)# aaa authentication mac primary radius secondary local
GA-MLxxTPoE+(config)#
```

11.1.12aaa authentication web

This command is used to configure the primary and secondary database, or auth-fail-action for web authentication. Use the **no** form of this command to revert to the default setting.

Syntax

- aaa authentication web {primary radius secondary {local | none} | primary local secondary {radius | none}}
- aaa authentication web auth-fail-action {secondary-db | stop}
- no aaa authentication web

Parameters

Parameters	Parameters auth-fail-action	Description
primary local secondary none (Default)	**secondary-db (Default)**	The authentication function will not operate. It will be treated as authentication approval, and communication will be allowed.
primary local secondary none or primary local secondary radius	**stop**	Only the local database will be used. If there is a denial in the local database, communication will be prohibited.
primary radius secondary none	**stop**	Only the RADIUS server will be used. If there is a denial on the RADIUS server, communication will be prohibited. If communication with the RADIUS server fails, it will be treated as authentication approval.
primary radius secondary local	**stop**	The RADIUS server will be used first. If there is a denial on the RADIUS server, communication will be prohibited. If communication with the RADIUS server fails, the local database will be used.
primary radius secondary local	**secondary-db**	The RADIUS server will be used first. If there is a denial on the RADIUS server, or if communication with the RADIUS server fails, the local database will be used.
primary local secondary radius	**secondary-db**	The local database will be used first. If there is a denial in the local database, the RADIUS server will be used.

Default

The authentication function will not operate.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to configure the primary and secondary database, or auth-fail-action for web authentication.

Example

This example shows how to set the primary database to use the RADIUS server and the secondary database to the local database for web authentication.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)# aaa authentication web primary radius secondary local
GA-MLxxTPoE+(config)#
```

11.1.13aaa group server radius

This command is used to enter the RADIUS group server configuration mode to associate server hosts with the group. Use the **no** form of this command to remove a RADIUS server group

Syntax

- **aaa group server radius** *GROUP-NAME*
- **no aaa group server radius** *GROUP-NAME*

Parameters

Parameters	Description
GROUP-NAME	Specifies the name of the server group. This name can be up to 32 characters long. The syntax is a general string that does not allow spaces.

Default

There is no AAA group server.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to define a RADIUS server group. The created server group is used in the definition of method lists used for authentication, or accounting by using the **aaa authentication** and **aaa accounting** commands. Also use this command to enter the RADIUS group server configuration mode. Use the **server** command to associate the RADIUS server hosts with the RADIUS server group.

Example

This example shows how to create a RADIUS server group with two entries. The second host entry acts as backup to the first entry.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#aaa group server radius group1
GA-MLxxTPoE+(config-sg-radius)# server 172.19.10.100
GA-MLxxTPoE+(config-sg-radius)# server 172.19.10.101
GA-MLxxTPoE+(config-sg-radius)#
```

11.1.14aaa group server tacacs+

This command is used to enter the TACACS+ group server configuration mode to associate server hosts with the group. Use the **no** form of this command to remove a TACACS+ server group

Syntax

- **aaa group server tacacs+** *GROUP-NAME*
- **no aaa group server tacacs+** *GROUP-NAME*

Parameters

Parameters	Description
GROUP-NAME	Specifies the name of the server group. This name can be up to 32 characters long. The syntax is a general string that does not allow spaces.

Default

There is no AAA group server.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to enter the TACACS+ group server configuration mode. Use the server command to associate the TACACS+ server hosts with the TACACS+ server group. The defined server group can be specified as the method list for authentication, or accounting by using the **aaa authentication** and **aaa accounting** commands.

Example

This example shows how to create a TACACS+ server group with two entries.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#aaa group server tacacs+ group1
GA-MLxxTPoE+(config-sg-tacacs+)# server 172.19.10.100
GA-MLxxTPoE+(config-sg-tacacs+)# server 172.19.11.20
GA-MLxxTPoE+(config-sg-tacacs+)#
```

11.1.15accounting commands

This command is used to configure the method list used for command accounting via a specific line. Use the **no** form of this command to disable do accounting command.

Syntax

- **accounting commands** *LEVEL* {**default** | *METHOD-LIST*}
- **no accounting commands** *LEVEL*

Parameters

Parameters	Description
LEVEL	Specifies to do accounting for all configure commands at the specified privilege level. The privilege level is between 1 and 15.
default	Specifies to do accounting based on the default method list.
METHOD-LIST	Specifies the name of the method list to use.

Default

By default, this option is disabled.

Command Mode

Line Configuration Mode

Command Default Level

Level: 15

Usage Guideline

For accounting via the method list to take effect, enable AAA first by using the **aaa new-model** command. Create the method list first by using the **aaa accounting commands** command. If the method list does not exist, the command does not take effect. The user can specify different method lists to account commands at different levels. A level can only have one method list specified.

Example

This example shows how to enable the command accounting level 15 configure command issued via the console using the accounting method list named "cmd-15" on the console.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# aaa accounting commands 15 cmd-15 start-stop group tacacs+
GA-MLxxTPoE+(config)# line console
GA-MLxxTPoE+(config-line)# accounting commands 15 cmd-15
GA-MLxxTPoE+(config-line)#
```

11.1.16accounting exec

This command is used to configure the method list used for EXEC accounting for a specific line. Use the **no** form of this command to disable the accounting EXEC option.

Syntax

- **accounting exec {default |** *METHOD-LIST*}
- **no accounting exec**

Parameters

Parameters	Description
default	Specifies to use the default method list.
METHOD-LIST	Specifies the name of the method list to use.

Default

By default, this option is disabled.

Command Mode

Line Configuration Mode

Command Default Level

Level: 15

Usage Guideline

For accounting via the method list to take effect, enable AAA first by using the **aaa new-model** command. Create the method list first by using the **aaa accounting exec** command. If the method list does not exist, the command does not take effect.

Example

This example shows how to configure the EXEC accounting method list with the name of "list-1". It uses the RADIUS server. If the security server does not response, it does not perform accounting. After the configuration, the EXEC accounting is applied to the console.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)# aaa accounting exec list-1 start-stop group radius
GA-MLxxTPoE+(config)# line console
GA-MLxxTPoE+(config-line)# accounting exec list-1
GA-MLxxTPoE+(config-line)#
```

11.1.17clear aaa counters servers

This command is used to clear the AAA server statistic counters.

Syntax

- **clear aaa counters servers** {**all** | **radius** {*IP-ADDRESS* | *IPV6-ADDRESS* | **all**} | **tacacs** {*IP-ADDRESS* | **all**} | **sg** *NAME*}

Parameters

Parameters	Description
all	Specifies to clear server counter information related to all server hosts.

Parameters	Description
radius *IP-ADDRESS*	Specifies to clear server counter information related to a RADIUS IPv4 host.
radius *IPV6-ADDRESS*	Specifies to clear server counter information related to a RADIUS IPv6 host.
radius all	Specifies to clear server counter information related to all RADIUS hosts.
tacacs *IP-ADDRESS*	Specifies to clear server counter information related to a TACACS IPv4 host.
tacacs all	Specifies to clear server counter information related to all TACACS hosts.
sg *NAME*	Specifies to clear server counter information related to all hosts in a server group.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to clear the statistics counter related to AAA servers.

Example

This example shows how to clear AAA server counters.

```
GA-MLxxTPoE+# clear aaa counters servers all
GA-MLxxTPoE+#
```

This example shows how to clear AAA server counters information for all hosts in the server group “server-farm”.

```
GA-MLxxTPoE+# clear aaa counters servers sg server-farm
GA-MLxxTPoE+#
```

11.1.18ip http accounting exec

This command is used to specify an AAA accounting method for HTTP server users. Use the **no** form of this command to revert to the default setting.

Syntax

- **ip http accounting exec** {**default** | *METHOD-LIST*}
- **no ip http accounting exec**

Parameters

Parameters	Description
default	Specifies to do accounting based on the default method list.
METHOD-LIST	Specifies the name of the method list to use.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

For accounting via the method list to take effect, enable AAA first by using the **aaa new-model** command. Create the method list first by using the **aaa accounting exec** command. If the method list does not exist, the command does not take effect.

Example

This example shows how to specify that the method configured for AAA should be used for accounting for HTTP server users. The AAA accounting method is configured as the RADIUS accounting method.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# aaa accounting exec list-1 start-stop group radius
GA-MLxxTPoE+(config)# ip http accounting exec list-1
GA-MLxxTPoE+(config)#
```

11.1.19 login authentication

This command is used to configure the method list used for login authentication via a specific line. Use the **no** form of this command to revert to the default method list.

Syntax

- **login authentication** {**default** | *METHOD-LIST*}
- **no login authentication**

Parameters

Parameters	Description
default	Specifies to authenticate based on the default method list.
METHOD-LIST	Specifies the name of the method list to use.

Default

By default, the default method list is used.

Command Mode

Line Configuration Mode

Command Default Level

Level: 15

Usage Guideline

For authentication via the method list to take effect, enable AAA first by using the **aaa new-model** command. Create the method list first by using the **aaa authentication login** command. If the method list does not exist, the command does not take effect and the authentication will be done via the default login method list.
When **aaa new-model** becomes enabled, the default method list is used for authentication.

Example

This example shows how to set the local console line to use the method list "CONSOLE-LINE-METHOD" for login authentication.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)# aaa authentication login CONSOLE-LINE-METHOD group group2 local
GA-MLxxTPoE+(config)# line console
GA-MLxxTPoE+(config-line)# login authentication CONSOLE-LINE-METHOD
GA-MLxxTPoE+(config-line)#
```

11.1.20 radius-server deadtime

This command is used to specify the default duration of the time to skip the unresponsive server. Use the **no** form of this command to revert to the default setting.

Syntax

- **radius-server deadtime** *MINUTES*
- **no radius-server deadtime**

Parameters

Parameters	Description
MINUTES	Specifies the dead time. The valid range is 0 to 1440 (24 hours). When the setting is 0, the unresponsive server will not be marked as dead.

Default

By default, this value is 0.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

This command can be used to improve the authentication processing time by setting the dead time to skip the unresponsive server host entries.

When the system performs authentication with the authentication server, it attempts one server at a time. If the attempted server does not respond, the system will attempt the next server. When the system finds a server does not respond, it will mark the server as down, start a dead time timer, and skip them in authentication of the following requests until expiration of the dead time.

Example

This example shows how to set the dead time to ten minutes.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)# radius-server deadtime 10
GA-MLxxTPoE+(config)#
```

11.1.21radius-server host

This command is used to create a RADIUS server host. Use the **no** form of this command to delete a server host.

Syntax

- **radius-server host** {*IP-ADDRESS* | *IPV6-ADDRESS*} [**auth-port** *PORT*] [**acct-port** *PORT*] [**timeout** *SECONDS*] [**retransmit** *COUNT*] **key** [**0** | **7**] *KEY-STRING*
- **no radius-server host** {*IP-ADDRESS* | *IPV6-ADDRESS*}

Parameters

Parameters	Description
IP-ADDRESS	Specifies the IP address of the RADIUS server.
IPV6-ADDRESS	Specifies the IPv6 address of the RADIUS server.
auth-port *PORT-NUMBER*	(Optional) Specifies the UDP destination port number for sending authentication packets. The range is 0 to 65535. Set the port number to zero if the server host is not for authentication purposes. The default value is 1812.
acct-port *PORT-NUMBER*	(Optional) Specifies the UDP destination port number for sending accounting packets. The range is 0 to 65535. Set the port number to zero if the server host is not for accounting purposes. The default value is 1813.
timeout *SECONDS*	(Optional) Specifies the server time-out value. The range of timeout is between 1 and 255 seconds. If not specified, the default value is 5 seconds.

Parameters	Description
retransmit *COUNT*	(Optional) Specifies the retransmit times of requests to the server when no response is received. The value is from 0 to 20. Use 0 to disable the retransmission. If not specified, the default value is 2.
0	(Optional) Specifies the password in clear text form. If not specified, this is the default option.
7	(Optional) Specifies the password in the encrypted form.
key *KEY-STRING*	Specifies the key used to communicate with the server. The key can between 1 and 32 clear text characters.

Default

By default, no server is configured.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to create RADIUS server hosts before it can be associated with the RADIUS server group using the server command.

Example

This example shows how to create two RADIUS server hosts with the different IP address.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)# radius-server host 172.19.10.100 auth-port 1500 acct-port 1501
timeout 8 retransmit 3 key ABCDE
GA-MLxxTPoE+(config)# radius-server host 172.19.10.101 auth-port 1600 acct-port 1601
timeout 3 retransmit 1 key ABCDE
GA-MLxxTPoE+(config)#
```

11.1.22server (RADIUS)

This command is used to associate a RADIUS server host with a RADIUS server group. Use the **no** form of this command to remove a server host from the server group.

Syntax

- **server** {*IP-ADDRESS* | *IPV6-ADDRESS*}
- **no server** {*IP-ADDRESS* | *IPV6-ADDRESS*}

Parameters

Parameters	Description
IP-ADDRESS	Specifies the IPv4 address of the authentication server.
IPV6-ADDRESS	Specifies the IPv6 address of the authentication server.

Default

By default, no server is configured.

Command Mode

RADIUS Group Server Configuration Mode

Command Default Level

Level: 15

Usage Guideline

Use the **aaa group server radius** command to enter the RADIUS group server configuration mode. Use this command to associate the RADIUS server hosts with the RADIUS server group. The defined server group can be specified as the method list for authentication, or accounting via the **aaa authentication** and **aaa accounting** commands. Use the **radius-server host** command to create a server host entry. A host entry is identified by IP Address.

Example

This example shows how to enter the RADIUS group server configuration mode and associate two RADIUS server hosts with the RADIUS server group.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#aaa group server radius group1
GA-MLxxTPoE+(config-sg-radius)# server 172.19.10.100
GA-MLxxTPoE+(config-sg-radius)# server 172.19.10.101
GA-MLxxTPoE+(config-sg-radius)#
```

11.1.23server (TACACS+)

This command is used to associate a TACACS+ server with a server group. Use the **no** form of this command to remove a server from the server group.

Syntax

- **server** *IP-ADDRESS*
- **no server** *IP-ADDRESS*

Parameters

Parameters	Description
IP-ADDRESS	Specifies the IPv4 address of the authentication server.

Default

By default, no host is in the server group.

Command Mode

TACACS+ Group Server Configuration Mode

Command Default Level

Level: 15

Usage Guideline

Use the **aaa group server tacacs+** command to enter the TACACS+ group server configuration mode. Use this command to associate the TACACS+ server hosts with the TACACS+ server group. The defined server group can be specified as the method list for authentication, or accounting via the **aaa authentication** and **aaa accounting** commands. The configured servers in the group will be attempted in the configured order. Use the **tacacs-server host** command to create a server host entry. A host entry is identified by the IP Address.

Example

This example shows how to create two TACACS+ server hosts. Then a server group is created with the two server hosts.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)# tacacs-server host 172.19.10.100 port 1500 timeout 8 key ABCDE
GA-MLxxTPoE+(config)# tacacs-server host 172.19.122.3 port 1600 timeout 3 key ABCDE
GA-MLxxTPoE+(config)#aaa group server tacacs+ group2
GA-MLxxTPoE+(config-sg-tacacs+)# server 172.19.10.100
GA-MLxxTPoE+(config-sg-tacacs+)# server 172.19.122.3
GA-MLxxTPoE+(config-sg-tacacs+)#
```

11.1.24show aaa

This command is used to display the AAA global state.

Syntax

- show aaa

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display the AAA global state.

Example

This example shows how to display the AAA global state.

```
GA-MLxxTPoE+# show aaa

AAA is enabled.

GA-MLxxTPoE+#
```

11.1.25 tacacs-server host

This command is used to create a TACACS+ server host. Use the **no** form of this command to remove a server host.

Syntax

- **tacacs-server host** *IP-ADDRESS* [**port** *PORT*] [**timeout** *SECONDS*] **key** [**0** | **7**] *KEY-STRING*
- **no tacacs-server host** *IP-ADDRESS*

Parameters

Parameters	Description
IP-ADDRESS	Specifies the IPv4 address of the TACACS+ server.
port *PORT-NUMBER*	(Optional) Specifies the UDP destination port number for sending request packets. The default port number is 49. The range is from 1 to 65535.
timeout *SECONDS*	(Optional) Specifies the time-out value. This value must be between 1 and 255 seconds. The default value is 5 seconds.
0	(Optional) Specifies the password in the clear text form. This is the default option.
7	(Optional) Specifies the password in the encrypted form.
key *KEY-STRING*	Specifies the key used to communicate with the server. The key can be from 1 to 254 clear text characters.

Default

No TACACS+ server host is configured.

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

Use the **tacacs-server host** command to create TACACS+ server hosts before it can be associated with the TACACS+ server group using the **server** command.

Example

This example shows how to create two TACACS+ server hosts with the different IP addresses.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)# tacacs-server host 172.19.10.100 port 1500 timeout 8 key ABCDE
GA-MLxxTPoE+(config)# tacacs-server host 172.19.122.3 port 1600 timeout 3 key ABCDE
GA-MLxxTPoE+(config)#
```

11.1.26 show aaa authentication auth-mac

This command is used to display the local user account for MAC authentication.

Syntax

- show aaa authentication auth-mac

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to display the local user account used for MAC authentication.

Example

This example shows how to display the local user account for MAC authentication.

```
GA-MLxxTPoE+#show aaa authentication auth-mac

Auth MAC Address  VLAN Filter-ID 2-Step Auth
----------------- ---- --------- -----------
00:01:02:03:04:05  100  3999      Any

GA-MLxxTPoE+#
```

11.1.27show aaa authentication auth-user

This command is used to display the local user account for 802.1X and web authentication.

Syntax

- show aaa authentication auth-user

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to display the local user account used for 802.1X and web authentication.

Example

This example shows how to display the local user account for 802.1X and web authentication.

```
GA-MLxxTPoE+#show aaa authentication auth-user

User Name             Password              VLAN Filter-ID Auth Type 2-Step Auth

--------------------- --------------------- ---- --------- --------- -----------
user                  [encrypted]           10   3999      802.1X    enable

GA-MLxxTPoE+#
```

11.1.28show aaa authentication dot1x

This command is used to display AAA settings for 802.1X authentication.

Syntax

- show aaa authentication dot1x

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to display AAA settings for 802.1X authentication.

Example

This example shows how to display AAA settings for 802.1X authentication.

```
GA-MLxxTPoE+#show aaa authentication dot1x

 Primary Database   : Local
 Secondary Database : None
 Auth Fail Action   : Stop

GA-MLxxTPoE+#
```

11.1.29show aaa authentication mac

This command is used to display AAA settings for MAC authentication.

Syntax

- show aaa authentication mac

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to display AAA settings for MAC authentication.

Example

This example shows how to display AAA settings for MAC authentication.

```
GA-MLxxTPoE+#show aaa authentication mac

 Primary Database     : Local
 Secondary Database   : None
 Auth Fail Action     : Secondary DB
 Auth Fail Block Time : 60 seconds

GA-MLxxTPoE+#
```

11.1.30 show aaa authentication web

This command is used to display AAA settings for web authentication.

Syntax

- show aaa authentication web

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to display AAA settings for web authentication.

Example

This example shows how to display AAA settings for web authentication.

```
GA-MLxxTPoE+#show aaa authentication web

 Primary Database       : Local       Auth Fail Action     : Secondary DB
 Secondary Database     : None        Auth Fail Block Time : 60    seconds

GA-MLxxTPoE+#
```

11.1.31 show radius statistics

This command is used to display RADIUS statistics for accounting and authentication packets.

Syntax

- show radius statistics

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display statistics counters related to servers.

Example

This example shows how to display the server related statistics counters.

```
GA-MLxxTPoE+#show radius statistics
RADIUS Server: 172.19.192.80: Auth-Port 1645, Acct-Port 1646
State is UP
                                Auth.   Acct.
Round Trip Time:                10      10
Access Requests:                 4      NA
Access Accepts:                  0      NA
Access Rejects:                  4      NA
Access Challenges:               0      NA
Acct Request:                   NA       3
Acct Response:                  NA       3
Retransmissions:                 0       0
Malformed Responses:             0       0
Bad Authenticators:              0       0
 Pending Requests:               0       0
 Timeouts:                       0       0
 Unknown Types:                  0       0
 Packets Dropped:                0       0
```

Display Parameters

Parameters	Description
Auth.	Statistics for authentication packets.
Acct.	Statistics for accounting packets.
Round Trip Time	The time interval (in hundredths of a second) between the most recent Response and the Request that matched it from this RADIUS server.
Access Requests	The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.

Parameters	Description
Access Accepts	The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
Access Rejects	The number of RADIUS Access-Reject packets (valid or invalid) received from this server.
Access Challenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
Acct Request	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.
Acct Response	The number of RADIUS packets received on the accounting port from this server.
Retransmissions	The number of RADIUS Request packets retransmitted to this RADIUS server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.
Malformed Responses	The number of malformed RADIUS Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or Signature attributes or unknown types are not included as malformed responses.
Bad Authenticators	The number of RADIUS Response packets containing invalid authenticators or Signature attributes received from this server.
Pending Requests	The number of RADIUS Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, a timeout or retransmission.
Timeouts	The number of timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
Unknown Types	The number of RADIUS packets of unknown type which were received from this server.
Packets Dropped	The number of RADIUS packets of which were received from this server and dropped for some other reason.

11.1.32 show tacacs statistics

This command is used to display the interoperation condition with each TACACS+ server.

Syntax

- show tacacs statistics

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display statistics counters related to servers.

Example

This example shows how to display the server related statistics counters.

```
GA-MLxxTPoE+# show tacacs statistics
TACACS+ Server: 172.19.192.80/49, State is UP
Socket Opens: 0
Socket Closes: 0
Total Packets Sent: 0
Total Packets Recv: 0
Reference Count: 0
```

Display Parameters

Parameters	Description
TACACS+ Server	IP address of the TACACS+ server.
Socket Opens	Number of successful TCP socket connections to the TACACS+ server.
Socket Closes	Number of successfully closed TCP socket attempts.
Total Packets Sent	Number of packets sent to the TACACS+ server.
Total Packets Recv	Number of packets received from the TACACS+ server.

Parameters	Description
Reference Count	Number of authentication requests from the TACACS+ server.

11.2 802.1X Commands

IEEE 802.1X provides user authentication when clients access the network and blocks connections to the network from unregistered clients. It prevents the access by unauthorized users or devices to protect information assets security.

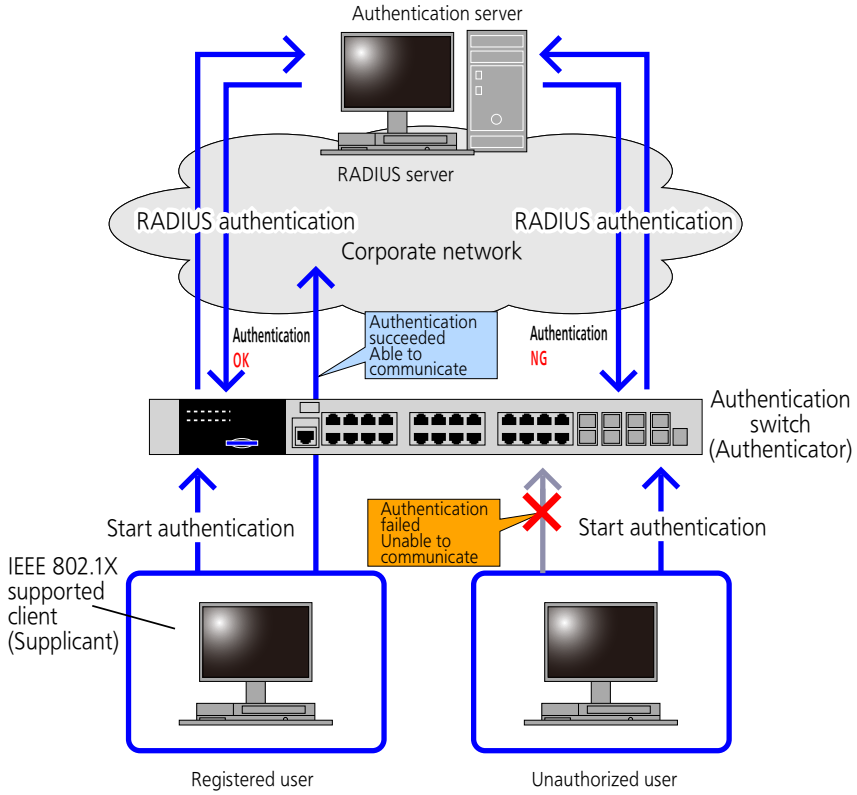


Figure 66-2 IEEE 802.1X overview

To use IEEE 802.1X authentication, there must be a client, an authentication switch, and an authentication server as illustrated in the diagram above.

- The client requires IEEE 802.1X compatible software (An IEEE 802.1X supported client is called Supplicant). The client sends an authentication request when connecting to the network and is able to access when authorized.
- The authentication switch intermediates an authentication process between the client and authentication server. It blocks connections to the network from unauthorized clients (The authentication switch is also called Authenticator). This switch allows you to enable/disable authentication for each port and configure the authentication settings.

- A RADIUS server is usually used for the authentication server. It only approves an authentication request from registered users. Up to three authentication servers can be registered in the authentication switch.

NOTE You can register users in a local database in the authentication switch and use the database in place of a RADIUS server or as a RADIUS server failover.

Port-based authentication and MAC-based authentication

You need to change the authentication method depending on how you connect the client to the port for the authentication switch. This switch allows you to select port-based or MAC-based authentication.

- **Port-based authentication:** Authorize a port to which the client is connected.
- **MAC-based authentication:** Authorize based on the MAC address of the client connected. It authorizes even in an environment where multiple clients communicate on a single port of the authentication switch (e.g. using an island hub). You can register up to 448 MAC addresses per port.

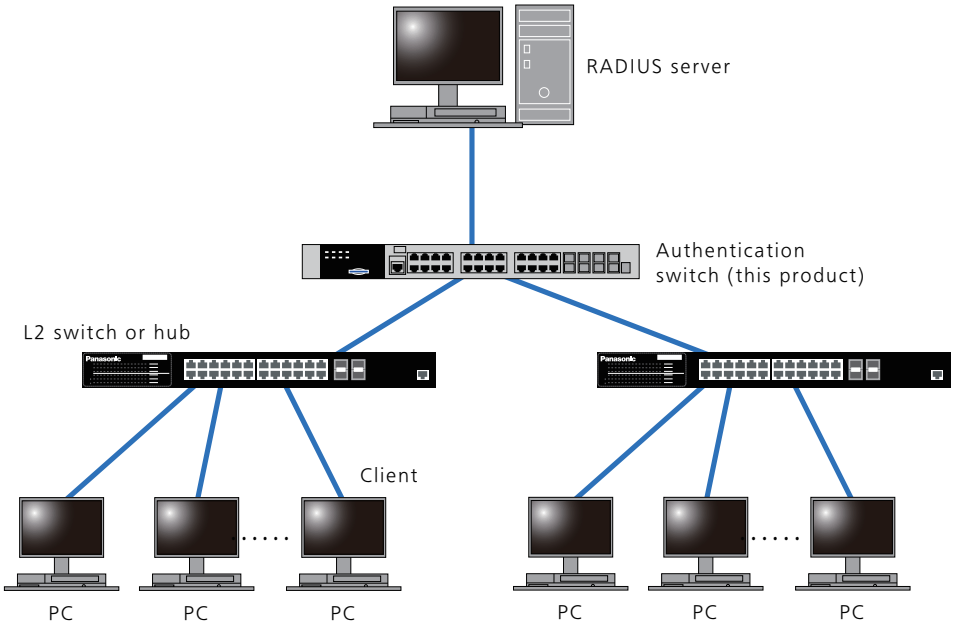


Figure 66-3 Authentication in island hub

NOTE For authentication in an island hub, a switch acting as an island hub requires the EAP packet forwarding function. An EAP frame is communication data used for an authentication process. If devices are connected via a switch not supporting the EAP packet forwarding function, EAP frames are discarded and authentication is not performed. (This switch supports the EAP packet forwarding function.)

Guest VLAN

Combining the IEEE 802.1X and guest VLAN functions allows for restricted access, such as authorizing connection to the Internet only instead of completely blocking communications from unauthorized clients.

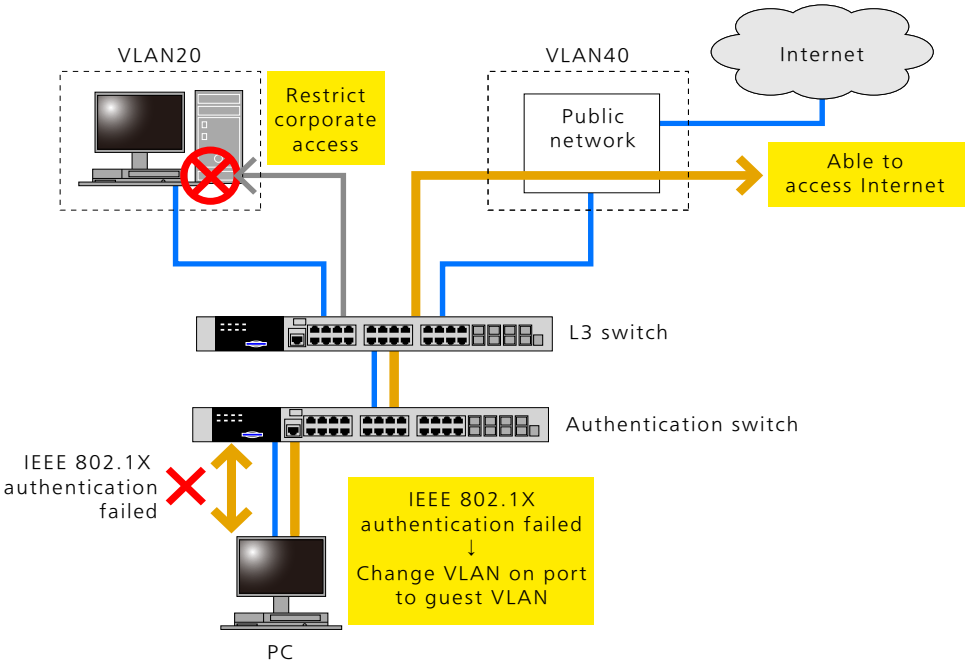


Figure 66-4 Connection through guest VLAN

NOTE Only one VLAN can be assigned to a guest VLAN.

Dynamic VLAN using IEEE 802.1X

In a static VLAN, the destination VLAN is fixed for each port. Meanwhile, in a dynamic VLAN, the destination VLAN is determined based on the client MAC address information regardless of a port to be connected.
There are several ways to configure dynamic VLAN. One of them is to use IEEE 802.1X RADIUS server information. If the client's VLAN information is registered in the RADIUS server, the VLAN information is retrieved during authentication, allowing for accessing the VLAN to which the client belongs from any port.

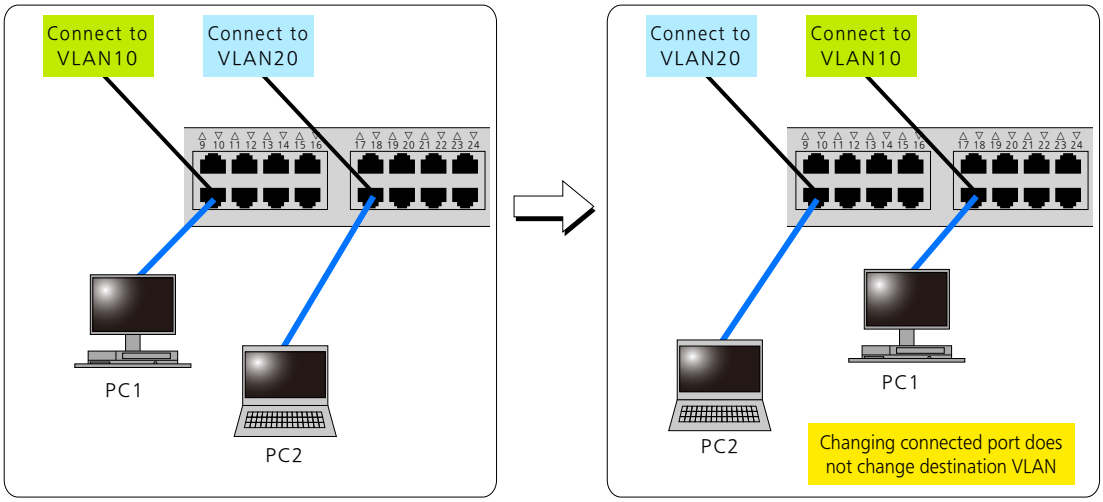


Figure 66-5 Dynamic VLAN

11.2.1 dot1x control-direction

This command is used to configure the direction of the traffic on a controlled port as unidirectional (in) or bidirectional (both).

Syntax

- dot1x control-direction {both | in}

Parameters

Parameters	Description
both	Specifies to enable bidirectional control for the port.
in	Specifies to enable in direction control for the port.

Default

By default, the bidirectional mode is used.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for physical port interface configuration. If the port control is set to **force-authorized**, then the port is not controlled in both directions. If the port control is set to **auto**, then the access to the port for the controlled direction needs to be authenticated. If the port control is set to **force-unauthorized**, then the access to the port for the controlled direction is blocked. Suppose that port control is set to **auto**. If the control direction is set to **both**, then the port can receive and transmit EAPOL packets only. All user traffic is blocked before authentication. If the control direction is set to **in**, then in addition to receiving and transmitting EAPOL packets, the port can transmit user traffic but not receive user traffic before authentication.

Example

This example shows how to configure the controlled direction of the traffic through Gigabit Ethernet 1/0/1 as unidirectional.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# dot1x control-direction in
GA-MLxxTPoE+(config-if)#
```

11.2.2 dot1x eap-request

This command is used to enable the EAP-Request function. Use the **no** form of this command to revert to the default setting.

Syntax

- **dot1x eap-request**
- **no dot1x eap-request**

Parameters

None

Default

By default, this function is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for physical port interface configuration. EAP-Request function is used to send unicast EAP continuously to invoke the sending of EAPoL-Start from the unauthorized host. If the host passed 802.1X authentication, its MAC address is deleted from the unauthorized MAC address table, and the Switch stops sending EAP.

Example

This example shows how to enable the EAP-Request function on Gigabit Ethernet 1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# dot1x eap-request
GA-MLxxTPoE+(config-if)#
```

11.2.3 dot1x eap-request interval

This command is used to revert the EAP-Request interval.

Syntax

- **dot1x eap-request interval** *SECONDS*

Parameters

Parameters	Description
SECONDS	Specifies the interval in seconds for the Switch to send unicast EAP to the unauthorized host. The value is from 1 to 3600.

Default

By default, the interval is 5 seconds.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

When security module settings can be applied to Link Aggregation port, this command is available for physical port and port channel interface configuration. Otherwise, this command is only available for physical port interface configuration.
This command is used to configure the EAP-Request interval for the switch to send unicast-EAP to the unauthorized host.

Example

This example shows how to configure the EAP-Request interval to 300 seconds.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# dot1x eap-request interval 300
GA-MLxxTPoE+(config)#
```

11.2.4 dot1x forceAuthorized mac

This command is used to set force authorized or unauthorized MAC on specific ports. Use the **no** form of this command to remove the specific entry or ports.

Syntax

- **dot1x forceAuthorized mac** *MAC-ADDRESS* **mask-bit** *INT* **auth-mode {authorized | unauthorized} interface** *INTERFACE-ID* **[, | -]**
- **no dot1x forceAuthorized mac** *MAC-ADDRESS* **interface** *INTERFACE-ID* **[, | -]**

Parameters

Parameters	Description
mac-address *MAC-ADDRESS*	Specifies the MAC address of the supplicant.
mask-bit *INT*	Specifies the mask bit length of MAC address. The value is from 0 to 48.
authorized	Specifies to force the authorized state.
unauthorized	Specifies to force the unauthorized state.
interface *INTERFACE-ID*	Specifies the port of the supplicant. Valid interfaces are physical ports.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for physical port interface configuration. This command is used to set a group of MAC addresses to force the authorized or unauthorized state on specific ports.
This command only takes effect on 802.1 X MAC-based ports.

Example

This example shows how to configure MAC group 00-01-02-03-04-XX to force authorized on Gigabit Ethernet 1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# dot1x forceAuthorized mac 00-01-02-03-04-00 mask-bit 40 auth-mode authorized interface gi1/0/1
GA-MLxxTPoE+(config)#
```

This example shows how to change MAC group 00-01-02-03-04-XX from Gigabit Ethernet 1/0/1 to Gigabit Ethernet 1/0/2.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# dot1x forceAuthorized mac 00-01-02-03-04-00 mask-bit 40 auth-mode authorized interface gi1/0/2
GA-MLxxTPoE+(config)# no dot1x forceAuthorized mac 00-01-02-03-04-00 interface gi1/0/1
GA-MLxxTPoE+(config)#
```

11.2.5 dot1x init

This command is used to initialize the authenticator state machine on a specific port.

Syntax

- **dot1x init**

Parameters

None

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to initialize the authenticator state machine of 802.1X port-based port.

Example

This example shows how to initialize the authenticator state machine on Gigabit Ethernet 1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# dot1x init
GA-MLxxTPoE+(config-if)#
```

11.2.6 dot1x mac-based init

This command is used to initialize the authenticator state machine on a specific port or associated with a specific MAC address.

Syntax

- **dot1x mac-based init** [*MAC-ADDRESS*]

Parameters

Parameters	Description
MAC-ADDRESS	(Optional) Specifies the MAC address to be initialized.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for physical port interface configuration.
Use the **dot1x mac-based init** command to initialize all authenticator state machines of 802.1X MAC-based ports.
Use the **dot1x mac-based init** *MAC-ADDRESS* command to initialize the specific authenticator state machine of 802.1X MAC-based ports.

Example

This example shows how to initialize all authenticator state machines on Gigabit Ethernet port 1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# dot1x mac-based init
GA-MLxxTPoE+(config-if)#
```

11.2.7 dot1x mac-based re-authenticate

This command is used to re-authenticate a specific port or MAC address.

Syntax

- **dot1x mac-based re-authenticate** [*MAC-ADDRESS*]

Parameters

Parameters	Description
MAC-ADDRESS	(Optional) Specifies the MAC address to be used.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for physical port interface configuration.
Use the **dot1x mac-based re-authenticate** command to re-authenticate all authenticator state machines of 802.1X MAC-based ports.
Use the **dot1x mac-based re-authenticate** *MAC-ADDRESS* command to re-authenticate the specific authenticator state machine of 802.1X MAC-based ports.

Example

This example shows how to re-authenticate MAC 00-01-02-03-04-05 to force authorized on Gigabit Ethernet 1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# dot1x mac-based re-authenticate 00-01-02-03-04-05
GA-MLxxTPoE+(config-if)#
```

11.2.8 dot1x mac-based re-authentication

This command is used to enable periodic re-authentication for a port or MAC address. Use the **no** form of this command to disable periodic re-authentication for a port or remove re-authentication configuration for a MAC address.

Syntax

- **dot1x mac-based re-authentication** [*MAC-ADDRESS*]
- **no dot1x mac-based re-authentication** [*MAC-ADDRESS*]

Parameters

Parameters	Description
MAC-ADDRESS	(Optional) Specifies the MAC address to be used.

Default

By default, this option is disabled and no MAC address is configured.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for physical port interface configuration.
Use the **dot1x mac-based re-authentication** command to enable periodic re-authentication for the specific port.
Use the **dot1x mac-based re-authentication** *MAC-ADDRESS* command to enable periodic re-authentication for the target MAC Address.

Port Re-Authentication State	MAC Re-Authentication State	Target MAC final Re-Authentication State
Enabled	Enabled	Enabled
Enabled	Not Configured	Enabled
Disabled	Enabled	Enabled
Disabled	Not Configured	Disabled

Use the **dot1x timeout re-authperiod** command to configure the interval in seconds between re-authentication attempts.

Example

This example shows how to enable MAC 00-01-02-03-04-05 periodic re-authentication on Gigabit Ethernet 1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# dot1x mac-based re-authentication 00-01-02-03-04-05
GA-MLxxTPoE+(config-if)#
```

11.2.9 dot1x max-req

This command is used to configure the maximum number of times that the backend authentication state machine will retransmit an Extensible Authentication Protocol (EAP) request frame to the supplicant before restarting the authentication process.

Syntax

- **dot1x max-req** *TIMES*

Parameters

Parameters	Description
TIMES	Specifies the number of times that the Switch retransmits an EAP frame to the supplicant before restarting the authentication process. The range is from 1 to 10.

Default

By default, this value is 2.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command is only available for physical port interface configuration. If no response to an authentication request from the supplicant within the timeout period (specified by the **dot1x timeout tx-period** *SECONDS* command), the Switch will retransmit the request. This command is used to specify the number of retransmissions.

Example

This example shows how to configure the maximum number of retries on Gigabit Ethernet 1/0/1 to be 3.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# dot1x max-req 3
GA-MLxxTPoE+(config-if)#
```

11.2.10dot1x nas-id

This command is used to configure the value of the NAS-Identifier (32) RADIUS attribute. Use the **no** form of this command to to clear NAS- Identifier value.

Syntax

- **dot1x nas-id** *STRING*

- no dot1x nas-id

Parameters

Parameters	Description
STRING	Specifies the string used for the NAS-Identifier (32) RADIUS attribute. The maximum length of the string is 16.

Default

The default string of NAS ID is “nas1”.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to configure the string of the NAS-Identifier attribute. NAS-Identifier is used in Access-Request packets to identify the NAS within the scope of the RADIUS server.

Example

This example shows how to configure the NAS-Identifier as “Sw01”.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# dot1x nas-id Sw01
GA-MLxxTPoE+(config)#
```

11.2.11dot1x port-auth-mode

This command is used to specify the 802.1X authentication mode.

Syntax

- dot1x port-auth-mode {port-based | mac-based}

Parameters

Parameters	Description
port-based	Specifies the port to operate in the port-based mode. Only a single authentication is performed and only this authorized host is allowed to access the network.
mac-based	Specifies the port to operate in the MAC-based mode. Each host will be authenticated individually.

Default

The default mode is port-based.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for physical port interface configuration.
When the port is operated in the port-based mode and only one of the hosts can be authenticated, this authorized host is allowed to access the port. According to 802.1X authentication, if the re-authentication fails or the authenticated user logs off, the port will be blocked for a quiet period. The port restores the processing of EAPOL packets after the quiet period.
When the port is operated in the MAC-based mode, each host needs to be authenticated individually to access the port. A host is represented by its MAC address. Only the authorized host is allowed to access.
After enabling the 802.1X global status using the **dot1x system-auth-control** command, use the **dot1x port-control auto** and **dot1x port-auth-mode port-based** commands to enable the 802.1X port-based authentication, or use the **dot1x port-auth-mode mac-based** command to enable the 802.1X mac-based authentication.

Example

This example shows how to specify Gigabit Ethernet 1/0/1 to operate in the MAC-based mode.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# dot1x port-auth-mode mac-based
GA-MLxxTPoE+(config-if)#
```

11.2.12 dot1x port-control

This command is used to control the authorization state of a port.

Syntax

- dot1x port-control {auto | force-authorized | force-unauthorized}

Parameters

Parameters	Description
auto	Specifies to enable IEEE 802.1X authentication for the port.
force-authorized	Specifies the port to the force authorized state.
force-unauthorized	Specifies the port to the force unauthorized state.

Default

By default, this option is set as force-authorized.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for physical port interface configuration.
This command takes effect when the 802.1X global status is enabled by using the dot1x system-auth-control command.
When the authorization state of the port is auto, access to the port needs to be authenticated in the controlled direction.
When the authorization state of the port is force-authorized, the port is not controlled in both directions.
When the authorization state of the port is force-unauthorized, access to the port is blocked in the controlled direction.

Example

This example shows how to configure the authorization state of Gigabit Ethernet 1/0/1 to force-unauthorized.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# dot1x port-control force-unauthorized
GA-MLxxTPoE+(config-if)#
```

11.2.13 dot1x re-authenticate

This command is used to re-authenticate a specific port.

Syntax

- dot1x re-authenticate

Parameters

None

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to re-authenticate a specific port When the port is configured as the port-based mode.

Example

This example shows how to re-authenticate Gigabit Ethernet 1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# dot1x re-authenticate
GA-MLxxTPoE+(config-if)#
```

11.2.14 dot1x re-authentication

This command is used to enable periodic re-authentication for a port. Use the **no** form of this command to disable periodic re-authentication for a port.

Syntax

- **dot1x re-authentication**
- **no dot1x re-authentication**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for physical port interface configuration.
Use the **dot1x re-authentication** command to enable periodic re-authentication for the specific port.
Use the **dot1x timeout re-authperiod** command to configure the interval in seconds between re-authentication attempts.

Example

This example shows how to enable periodic re-authentication on Gigabit Ethernet 1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# dot1x re-authentication
GA-MLxxTPoE+(config-if)#
```

11.2.15 dot1x re-auth-timer local

This command is used to enable the local timer to re-authenticate a session. Use the no form of this command to revert to the default setting.

Syntax

- dot1x re-auth-timer local
- no dot1x re-auth-timer local

Parameters

None

Default

By default, the value of the RADIUS Session-Timeout attribute (27) is used for the timer to re-authenticate a session.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for physical port interface configuration.
This command is used to configure the local timer to re-authenticate a session. When the value of the RADIUS Termination-Action attribute (29) is RADIUS-Request (1), 802.1X will re-authenticate the host When the value of the RADIUS Termination-Action attribute (29) is Default (0), the session terminates.

Example

This example shows how to enable the local timer to re-authenticate a session.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# dot1x re-auth-timer local
GA-MLxxTPoE+(config-if)#
```

11.2.16dot1x statistics reset

This command is used to clear the 802.1X statistics.

Syntax

- dot1x statistics reset

Parameters

None

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to clear the 802.1X statistics.

Example

This example shows how to clear the 802.1X statistics.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# dot1x statistics reset
GA-MLxxTPoE+(config)#
```

11.2.17dot1x supplicant-num

This command is used to configure the maximum number of 802.1X authenticated users for a specific port.

Syntax

- dot1x supplicant-num *NUMBER*

Parameters

Parameters	Description
NUMBER	Specifies the maximum number of 802.1X authenticated users. The range is from 1 to 512.

Default

By default, there is no limit.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to configure the maximum number of 802.1X authenticated users for a specific port. The users are limited to 802.1X users. If the maximum number of 802.1X authenticated users is less than the current 802.1X authenticated users, this command will be rejected.

Example

This example shows how to configure the maximum number of 802.1X authenticated users on Gigabit Ethernet 1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# dot1x supplicant-num 256
GA-MLxxTPoE+(config-if)#
```

11.2.18dot1x system-auth-control

This command is used to globally enable IEEE 802.1X authentication on the Switch. Use the **no** form of this command to disable IEEE 802.1X authentication.

Syntax

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

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The 802.1X authentication function restricts unauthorized hosts from accessing the network. Use the **dot1x system-auth-control** command to globally enable the 802.1X authentication control. When 802.1X authentication is enabled, the system will authenticate the 802.1X user based on the method list configured by the **aaa authentication dot1x default** command.

Example

This example shows how to enable IEEE 802.1X authentication globally on the Switch.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# dot1x system-auth-control
GA-MLxxTPoE+(config)#
```

11.2.19dot1x timeout

This command is used to configure the IEEE 802.1X timers.

Syntax

- **dot1x timeout {quiet-period | re-authperiod | server | supp-timeout | tx-period | force-authorized-mac}** *SECONDS*

Parameters

Parameters	Description
quiet-period *SECONDS*	Specifies the number of seconds that the Switch will be in the quiet state in the wake of a failed authentication process. The range is from 1 to 65535.
re-authperiod *SECONDS*	Specifies the number of seconds between re-authentication attempts. The range is from 1 to 65535.
server *SECONDS*	Specifies the number of seconds that the Switch will wait for the request from the authentication server before timing out the server. On timeout, the authenticator will send an EAP-Request packet to the client. The range is from 1 to 65535.
supp-timeout *SECONDS*	Specifies the number of seconds that the Switch will wait for the response from the supplicant before timing out supplicant messages other than the EAP request ID. The range is from 1 to 65535.
tx-period *SECONDS*	Specifies the number of seconds that the Switch will wait for a response to an EAP-Request/Identity frame from the supplicant before retransmitting the request. The range is from 1 to 65535.
force-authorized-mac *SECONDS*	Specifies the number of seconds that the Switch will wait for the timeout of the force-authorized or force-unauthorized entry. The range is 0 to 65535. 0 represents never timeout.

Default

The **quiet-period** is 60 seconds.
The **re-authperiod** is 3600 seconds.
The **server** is 30 seconds.
The **supp-timeout** is 30 seconds.
The **tx-period** is 30 seconds.
The **force-authorized-mac** is 3600 seconds.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for physical port interface configuration.

Example

This example shows how to configure the server timeout value, supplicant timeout value, and the TX period on Gigabit Ethernet port 1/0/1 to be 15, 15, and 10 seconds, respectively.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# dot1x timeout server-timeout 15
GA-MLxxTPoE+(config-if)# dot1x timeout supp-timeout 15
GA-MLxxTPoE+(config-if)# dot1x timeout tx-period 10
GA-MLxxTPoE+(config-if)#
```

11.2.20 dot1x unauthorized age-out time

This command is used to set the age-out time of static unauthorized hosts.

Syntax

- **dot1x unauthorized age-out time** *SECONDS*

Parameters

Parameters	Description
SECONDS	Specifies the age-out time value in seconds. The range is from 0 to 65535. 0 represents never timeout.

Default

By default, the time is 300 seconds.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

When the security module settings can be applied to Link Aggregation port, this command is available for physical port and port channel interface configuration. Otherwise, this command is only available for physical port interface configuration.

This command is used to set the age-out time of static unauthorized hosts that are configured by the **dot1x unauthorized mac** command.

Example

This example shows how to set the age-out time of static unauthorized hosts to 1000 seconds.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# dot1x unauthorized age-out time 1000
GA-MLxxTPoE+(config)#
```

11.2.21 dot1x unauthorized mac

This command is used to add an 802.1X static unauthorized entry for the EAP-Request function. Use the **no** form of this command to remove the static unauthorized entry.

Syntax

- **dot1x unauthorized mac** *MAC-ADDRESS* **interface** *INTERFACE-ID*
- **no dot1x unauthorized mac** *MAC-ADDRESS*

Parameters

Parameters	Description
MAC-ADDRESS	Specifies the MAC address of the unauthorized host.
interface *INTERFACE-ID*	Specifies the port that the unauthorized host resides in.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for physical port interface configuration. This command is used to add or remove an 802.1X static unauthorized entry for the EAP-Request function. The static entry is removed at the next age-out time.

Example

This example shows how to add the unauthorized host, 00-01-02-03-04-05, on Gigabit Ethernet 1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# dot1x unauthorized mac 00-01-02-03-04-05 interface gi1/0/1
GA-MLxxTPoE+(config)#
```

11.2.22 eap-forward

This command is used to enable the forwarding of dot1x PDU. Use the **no** form of this command to disable the forwarding of dot1x PDU.

Syntax

- **eap-forward**
- **no eap-forward**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for physical port interface configuration.

This command only takes effect when the dot1x authentication function is disabled on the receiving port. The received PDU will be forwarded in either tagged or untagged form based on the VLAN setting.

Example

This example shows how to enable the forwarding of dot1x PDU.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# eap-forward
GA-MLxxTPoE+(config-if)#
```

11.2.23 show dot1x

This command is used to display the IEEE 802.1X authentication information of the specified interface.

Syntax

- **show dot1x {port-based interface** *INTERFACE-ID* **[, | -] | mac-based interface interface** *INTERFACE-ID*}

Parameters

Parameters	Description
interface *INTERFACE-ID*	Specifies to display the dot1x configuration on the specified interface or range of interfaces.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to display 802.1X port-based or MAC-based authentication information.

Example

This example shows how to display the dot1X port-based information on Gigabit Ethernet 1/0/2.

```
GA-MLxxTPoE+# show dot1x port-based interface gi1/0/2

 NAS ID: nas1

 Port No: Gi1/0/2   Authorized MAC Address: 00-19-5B-E9-5C-A7
 Port Status       : Authorized            OperControlDirection : Both
 Port Control      : Auto                  AdminControlDirection: Both
 Quiet Period      : 60    seconds         Transmission Period  : 30    seconds
 Supplicant Timeout: 30    seconds         Server Timeout       : 30    seconds
 Maximum Request   : 2                     Re-auth Period       : 3600  seconds
 Per Port Re-auth  : Disabled              Current PVID         : 1
 Guest VLAN ID     : ----                  Default VLAN ID      : ----
 Re-Auth Timer Mode: RADIUS


GA-MLxxTPoE+#
```

This example shows how to display the dot1X MAC-based information on Gigabit Ethernet 1/0/2.

```
GA-MLxxTPoE+# show dot1x mac-based interface gi1/0/2

 NAS ID: nas1            Port No: Gi1/0/2  Number of Supplicant: 512
 OperControlDirection: Both             AdminControlDirection   : Both
 Transmission Period : 30    seconds    Maximum Request         : 2
 Supplicant Timeout  : 30    seconds    Quiet Period            : 60    seconds
 Server Timeout      : 30    seconds    Re-authentication Period: 3600  seconds
 Force Auth Timeout  : 3600  seconds    Per Port Re-auth        : Disabled
 Re-Auth Timer Mode  : RADIUS
 Supplicant MAC Addr  Type      MAC Control     Auth Status  Re-auth
 ------------------- ------- ------------------ ------------ --------
 00-19-5B-E9-5C-A7   Dynamic Auto               Authorized   Disabled


GA-MLxxTPoE+#
```

11.2.24show dot1x eap-request port config

This command is used to display the 802.1X EAP-Request function.

Syntax

- show dot1x eap-request port config

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to display the 802.1X EAP-Request function.

Example

This example shows how to display the 802.1X EAP-Request function.

```
GA-MLxxTPoE+#show dot1x eap-request port config

 EAP-Request Interval:    5 Sec.

 Port    EAP-Request
 ------  ------------
   1       Enabled
   2       Disabled
   3       Disabled
   4       Disabled
   5       Disabled
   6       Disabled

GA-MLxxTPoE+#
```

11.2.25show dot1x forceAuthorized-MAC

This command is used to display force authorized or unauthorized entries.

Syntax

- **show dot1x forceAuthorized-MAC {all | single** *MAC-ADDRESS* **}**

Parameters

Parameters	Description
all	Specifies to display all force authorized or unauthorized entries.
single *MAC-ADDRESS*	Specifies to display the specific force authorized or unauthorized entry.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to display force authorized or unauthorized entries.

Example

This example shows how to display force authorized or unauthorized entries.

```
GA-MLxxTPoE+#show dot1x forceAuthorized-MAC all

 MAC Address        Mask  Auth Status   Port List
 -----------------  ----  ------------  -------------------------
 00-01-02-03-04-00  40    Authorized    Gi1/0/20-1/0/24

GA-MLxxTPoE+#
```

11.2.26 show dot1x statistics

This command is used to display IEEE 802.1X statistics.

Syntax

- **show dot1x statistics interface** *INTERFACE-ID* **{since-reset | since-up}**

Parameters

Parameters	Description
interface *INTERFACE-ID*	Specifies to display the dot1x statistics on the specified interface.
since-reset	Specifies to display the dot1x statistics since the last system reset.
since-up	Specifies to display the dot1x statistics since the device booted up.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to display IEEE 802.1X statistics since the last system reset or device booted up.

Example

This example shows how to display the dot1x statistics since last device booted up on Gigabit Ethernet 1/0/2.

```
GA-MLxxTPoE+# show dot1x statistics interface gi1/0/2 since-up

 Port: Gi1/0/2 Elapsed Time Since System Up: 000:04:19:25
 <Counter Name>           <Total>
 TxReqId                    5
 TxReq                      6
 TxTotal                    15
 RxStart                    1
 RxLogoff                   0
 RxRespId                   3
 RxResp                     6
 RxInvalid                  0
 RxLenError                 0
 RxTotal                    10
 RxVersion                  1
 LastRxSrcMac               00-19-5B-E9-5C-A7

GA-MLxxTPoE+#
```

11.2.27show dot1x unauthorized mac-address-table

This command is used to display the 802.1X unauthorized host table.

Syntax

- **show dot1x unauthorized mac-address-table {interface** *INTERFACE-ID* **[, | -] | mac}**

Parameters

Parameters	Description
interface *INTERFACE-ID*	Specifies to display the dot1x unauthorized hosts on the specified interface or range of interfaces.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
mac	Specifies to display the dot1x unauthorized hosts sorted by their MAC address.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to display the 802.1X unauthorized host table. The table inclues static unauthorized hosts that is manually configured and dynamic unauthorized hosts.

Example

This example shows how to display dot1X unauthorized hosts sorted by their MAC address.

```
GA-MLxxTPoE+# show dot1x unauthorized mac-address-table mac

 Age-Out Time:   300 Sec.
 MAC Address         Port
 -----------------   ---------
 00-01-02-03-04-05   Gi1/0/24
 00-19-5B-E9-5C-A7   Gi1/0/24

GA-MLxxTPoE+#
```

11.3 MAC Authentication Commands

11.3.1 mac-authentication

This command is used to enable MAC authentication globally. Use the **no** form of this command to disable the MAC authentication globally.

Syntax

- **mac-authentication**
- **no mac-authentication**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

MAC authentication is a feature designed to authenticate a user by MAC address when the user is trying to access the network via the Switch. The Switch itself can perform the authentication based on a local database or be a RADIUS client and perform the authentication process via the RADIUS protocol with a remote RADIUS server.

Example

This example shows how to enable MAC authentication globally.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# mac-authentication
GA-MLxxTPoE+(config)#
```

11.3.2 mac-authentication auth-fail block-time

This command is used to configure the blocking time after a MAC authentication request is rejected at the specific port.

Syntax

- **mac-authentication auth-fail block-time** *SECONDS*

Parameters

Parameters	Description
block-time *SECONDS*	Specifies the blocking time after a MAC authentication request is rejected at the specific port. The value is from 1 to 65535

Default

By default, the blocking time is 60 seconds.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to configure the blocking time after a MAC authentication request is rejected at the specific port

Example

This example shows how to configure the blocking time to 600 seconds.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#mac-authentication auth-fail block-time 600
GA-MLxxTPoE+(config)#
```

11.3.3 mac-authentication mac-format

This command is used to configure the MAC address format that will be used for authenticating as the username via the RADIUS server.

Syntax

- **mac-authentication mac-format case {upper | lower} delimiter {hyphen | colon | dot | none} delimited-char-num {2 | 4 | 6}**

Parameters

Parameters	Description
case	**upper:** Specifies that when using uppercase format, the RADIUS authentication username will be formatted as: AA-BB-CC-DD-EE-FF. **lower:** Specifies that when using the lowercase format, the RADIUS authentication username will be formatted as: aa-bb-cc-dd-ee-ff.
delimiter	**hyphen:** Specifies that when using "-"as delimiter, the format is: AA-BB-CC-DD-EE-FF. **colon:** Specifies that when using ":"as delimiter, the format is: AA:BB:CC:DD:EE:FF. **dot:** Specifies that when using "."as delimiter, the format is: AA.BB.CC.DD.EE.FF. **none:** Specifies that when not using any delimiter, the format is: AABBCCDDEEFF.
delimiter-char-num	Specifies the delimiter number value. Choose one of the following delimiter options: **2:** Single delimiter, the format is: AA-BB-CC-DD-EE-FF. **4:** Double delimiters, the format is: AABB-CCDD-EEFF. **6:** Multiple delimiters, the format is: AABBCC-DDEEFF. If **none:** is chosen for delimiter, the number does not take effect.

Default

The default authentication MAC address case is upper.
The default authentication MAC address delimiter is hyphen.
The default authentication MAC address delimiter number is 6.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to configure the formatting of usernames used for RADIUS authentication or for IGMP security based on the MAC address.

Example

This example shows how to format the username based on the MAC address.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# mac-authentication mac-format case upper delimiter hyphen
delimited-char-num 4
GA-MLxxTPoE+(config)#
```

11.3.4 mac-authentication password type

This command is used to configure the password type for MAC authentication.

Syntax

- **mac-authentication password type {mac | manual}**

Parameters

Parameters	Description
mac	Specifies to use MAC address as the password.
manual	Specifies to use manual string as the password.

Default

By default, MAC address is used.

Command Mode

Global Configuration Mode,

Command Default Level

Level: 12

Usage Guideline

This command is used to configure the password type for MAC authentication.

Example

This example shows how to configure to use manual string as the password.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#mac-authentication password type manual
GA-MLxxTPoE+(config)#
```

11.3.5 mac-authentication password manual

This command is used to configure the password for MAC authentication when the password type is configured as manual. Use the **no** form of this command to revert to the default setting.

Syntax

- **mac-authentication password manual** *STRING*
- **no mac-authentication password manual**

Parameters

Parameters	Description
STRING	Specifies to set the password for MAC authentication. The length of the string is between 1 and 32 characters.

Default

By default, the password is blank (empty string).

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to configure the password for MAC authentication when the password type is configured as **manual.**

Example

This example shows how to configure the password to be 123.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#mac-authentication password manual 123
GA-MLxxTPoE+(config)#
```

11.3.6 mac-authentication interface

This command is used to enable MAC authentication on the specified interface. Use the **no** form of this command to disable MAC authentication.

Syntax

- **mac-authentication interface** *INTERFACE-ID* **[,| -]**
- **no mac-authentication interface**

Parameters

Parameters	Description
INTERDACE-ID	Specifies the interfaces to be used.
,	(Optional) Specifies a series of interfaces or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to enable MAC authentication on the specified interface.

Example

This example shows how to enable MAC authentication on Gigabit Ethernet 1/0/1-8.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#mac-authentication interface gi1/0/1-8
GA-MLxxTPoE+(config)#
```

11.3.7 show mac-authentication

This command is used to display settings of MAC authentication.

Syntax

- **show mac-authentication**

Parameters

None

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to display settings of MAC authentication.

Example

This example shows how to display settings of MAC authentication.

```
GA-MLxxTPoE+#show mac-authentication

MAC Address Format for RADIUS Username
 Case                    :Upper
 Delimiter               :Hyphen
 Delimiter Characters    :4

RADIUS Password Type :Manual
Manual Password      :123

GA-MLxxTPoE+#
```

11.3.8 snmp-server enable traps mac-auth

This command is used to enable the sending of SNMP notifications for MAC authentication. Use the **no** form of this command to disable the sending of SNMP notifications.

Syntax

- **snmp-server enable traps mac-auth**
- **no snmp-server enable traps mac-auth**

Parameters

None

Default

By default, this feature is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

None

Example

This example shows how to enable the sending of traps for MAC authentication.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# snmp-server enable traps mac-auth
GA-MLxxTPoE+(config)#
```

11.4 Web Authentication Commands

11.4.1 web-authentication interface

This command is used to enable the Web authentication function on the port. Use the **no** form of this command to disable the Web authentication function.

Syntax

- **web-authentication interface** *INTERFACE-ID* [,|-]
- **no web-authentication interface**

Parameters

Parameters	Description
interface *INTERFACE-ID*	Specifies the interfaces to be used.
,	(Optional) Specifies a series of interfaces or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allow before and after the hyphen.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command allows hosts connected to the port to do authentication via the Web browser.

Example

This example shows how to enable the Web authentication function on GigabitEthernet1/0/1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#web-authentication interface gi1/0/1
GA-MLxxTPoE+(config)#
```

11.4.2 web-authentication contents

This command is used to customize the Web authentication page elements. Use the **no** form of this command to return to the default setting.

Syntax

- **web-authentication contents** {**description** *STRING* | **message** *STRING* | **password** *STRING* | **title** *STRING* | **username** *STRING*}
- **no web-authentication contents** {**description** | **message** | **password** | **title** | **username** | **logo-data**}

Parameters

Parameters	Description
title *STRING*	Specifies the title of the Web authentication page. The maximum number can be up to 64 characters.
username *STRING*	Specifies the user name title of Web authentication login window. The maximum number can be up to 32 characters.
password *STRING*	Specifies the password title of Web authentication login window. The maximum number can be up to 32 characters.
message *STRING*	Specifies the message field of the Web authentication login window. The maximum number can be up to 256 characters.
description *STRING*	Specifies the description field of Web authentication login window. The maximum number can be up to 256 characters.
logo-data	Specifies the copyright information by lines in Web authentication pages. The total copyright information can be up to 5 lines and 128 characters for each line.

Default

By default, the description field is not set.
By default, the message field is not set.
By default, the password title is “Password”.

By default, the title is not set.
By default, the username title is “User Name”.
By default, the log file does not exist.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Administrators can customize Web authentication page elements.

Example

This example shows how to configure the title to Panasonic.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#web-authentication contents title Panasonic
GA-MLxxTPoE+(config)#
```

11.4.3 web-authentication redirect

This command is used to configure the default URL the client Web browser will be redirected to after successful authentication. Use the **no** form of this command to remove the specification.

Syntax

- **web-authentication redirect** *STRING*
- **no web-authentication redirect**

Parameters

Parameters	Description
STRING	Specifies the default URL the client Web browser will be redirected to after successful authentication. If no default redirect URL is specified, the Web authentication logout page will be displayed. The default redirect path can be up to 64 characters.

Default

By default, the Web authentication logout page is displayed.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to specify the Web page to display to the hosts who passes the Web authentication.

Example

This example shows how to configure the default redirect path to be "http://www.website.com" after passing Web authentication.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# web-authentication redirect http://www.website.com
GA-MLxxTPoE+(config)#
```

11.4.4 web-auth system-auth-control

This command is used to enable the Web authentication function globally. Use the **no** form of this command to disable the function.

Syntax

- **web-authentication**
- **no web-authentication**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Web-based Authentication is used to authenticate users who access the Internet using Web browsers through the Switch. The switch itself can be the authentication server and do the authentication based on a local database, or be a RADIUS client and perform the authentication process via RADIUS protocol with the remote RADIUS server.The authentication process uses HTTP protocol.

Example

This example shows how to enable the Web authentication function globally.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#web-authentication
GA-MLxxTPoE+(config)#
```

11.4.5 web-authentication virtual-ip

This command is used to configure the Web authentication virtual IP address which is used to accept authentication requests from host. Use the **no** form of this command to revert to the default setting.

Syntax

- **web-authentication virtual-ip** {*IP-ADDRESS*}
- **no web-authentication virtual-ip**

Parameters

Parameters	Description
IP-ADDRESS	Specifies the Web authentication virtual IPv4 address.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The virtual IP of Web authentication is just the characterization of the Web authentication function on the Switch. All Web authentication processes communicate with this IP address, however, the virtual IP does not respond to any ICMP packet or ARP request. So it's not allowed to configure virtual IP in the same subnet as the Switch's IP interface or the same subnet as the host PCs' subnet, otherwise the Web authentication cannot operate correctly.
The defined URL only takes effect when the virtual IP address is configured. The users get the FQDN URL stored on the DNS server to get the virtual IP address. The obtained IP address must match the virtual IP address configured by the command.
If the IPv4 virtual IP is not configured, the IPv4 access cannot start a Web authentication.

Example

This example shows how to configure the Web authentication virtual IP to be "1.1.1.1".

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# web-authentication virtual-ip 1.1.1.1
GA-MLxxTPoE+(config)#
```

11.4.6 web-authentication web-port

This command is used to configure the HTTP port used for web authentication on the Switch. Use the **no** form of this command to revert to the default setting.

Syntax

- **web-authentication web-port http** *TCP-PORT*
- **no web-authentication web-port http**

Parameters

Parameters	Description
TCP-PORT	Specifies the TCP port for web authentication. The value is from 1 to 65535.

Default

By default the HTTP port number is 80.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to configure the HTTP port used for web authentication on the Switch. The HTTP packets from the TCP port is trapped to the CPU for authentication, or to access the login page.

Example

This example shows how to configure the TCP port as 8888.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#web-authentication web-port http 8888
GA-MLxxTPoE+(config)#
```

11.4.7 web-authentication auth-fail block-time

This command is used to configure the block time for web authentication.

Syntax

- **web-authentication auth-fail block-time** *SECONDS*

Parameters

Parameters	Description
SECONDS	Specifies the time in seconds to be blocked. The value is from 1 to 65535.

Default

60 seconds.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to configure the block time after the login is failed for 3 times. During the block time, the login is not permitted.

Example

This example shows how to configure the block time to 100 seconds.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#web-authentication auth-fail block-time 100
GA-MLxxTPoE+(config)#
```

11.4.8 show web-authentication

This command is used to display the web authentication settings.

Syntax

- **show web-authentication**

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display the web authentication settings.

Example

This example shows how to display the web authentication settings..

```
GA-MLxxTPoE+#show web-authentication

 Virtual IP Address : 172.10.1.1
 HTTP Port Number   : 8888
 Redirect URL       :

GA-MLxxTPoE+#
```

11.4.9 show web-authentication contents

This command is used to display the elements of web authentication page.

Syntax

- **show web-authentication contents**

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display the web authentication settings.

Example

This example shows how to display the elements of web authentication page...

```
GA-MLxxTPoE+#show web-authentication contents

 Page title          :
 Logo Data           : None
 User Name String    : User Name
 Password String     : Password
 Message             :
 Description         :

GA-MLxxTPoE+#
```

11.4.10copy tftp logo-data

This command is used to upload the logo file for web authentication.

Syntax

- copy tftp: *//LOCATINO/FILE-NAME* logo-data

Parameters

Parameters	Description
IP-ADDRESS	Specifies the IP address of the TFTP server.
FILE-NAME	Specifies the file name of the logo. The supported file format are JPG, PNG, and GIF. The file size is limited up to 512KB.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to upload the logo file for web authentication.

Example

This example shows how to upload the logo file for web authentication..

```
GA-MLxxTPoE+# copy tftp: //10.90.90.23/wac.jpg logo-data
Address of remote host [10.90.90.23]?
Source filename [wac.jpg]?
 Accessing tftp://10.90.90.23/wac.jpg...
 Transmission start...
 Transmission finished, file length 21909 bytes.
 Logo type is JPG.
 Please wait, programming flash.............. Done

GA-MLxxTPoE+#
```

11.5 Authentication Commands

11.5.1 authentication aging-time

This command is used to configure the aging timer for MAC authentication sessions.

Syntax

- **authentication aging-time** *MINUTES*

Parameters

Parameters	Description
MINUTES	Specifies the timer in minutes. The range is from 0 to 65535.

Default

The default timer is 1440 minutes.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to configure the aging timer for MAC authentication sessions. This command is not available for 802.1X.

Example

This example shows how to configure the aging timer to 200.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)# authentication aging-time 200
GA-MLxxTPoE+(config)#
```

11.5.2 authentication default-vlan

This command is used to configure the authentication default VLAN setting. Use the **no** form of this command to remove the authentication default VLAN.

Syntax

- **authentication default-vlan** *VLAN-ID*
- **no authentication default-vlan**

Parameters

Parameters	Description
VLAN-ID	Specifies the VLAN as the authentication default VLAN.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The specified VLAN must exist as a static VLAN before configuring it as the authentication default VLAN. This command is available for physical port interface configuration.
After the host passes authentication, it will be assigned to the default VLAN when the dynamic VLAN is disabled or the target VLAN is invalid. However, the host will stay in the original received VLAN if the default VLAN is invalid.

Example

This example shows how to configure VLAN 5 as the authentication default VLAN.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/4
GA-MLxxTPoE+(config-if)#authentication default-vlan 5
GA-MLxxTPoE+(config-if)#
```

11.5.3 authentication dynamic-vlan radius-attribute

This command is used to enable the acceptance of the authorized configuration. Use the **no** form of this command disable the function.

Syntax

- **authentication dynamic-vlan radius-attribute**
- **no authentication dynamic-vlan radius-attribute**

Parameters

None

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The command is used to enable or disable the acceptance of the authorized configuration. When enabled, the authorized attributes such as VLAN, 802.1p default priority, bandwidth, and ACL that are assigned by the RADIUS server will be accepted.
Bandwidth and ACL are assigned on port-basis. If authentication on the Switch is in the mac-based mode, VLAN and 802.1p are assigned on host-basis.

Example

This example shows how to disable the authrozation status.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#no authentication dynamic-vlan radius-attribute
GA-MLxxTPoE+(config)#
```

11.5.4 authentication guest-vlan

This command is used to configure the authentication guest VLAN setting. Use the **no** form of this command to remove the authentication guest VLAN.

Syntax

- **authentication guest-vlan** *VLAN-ID*
- **no authentication guest-vlan**

Parameters

Parameters	Description
VLAN-ID	Specifies the VLAN as the authentication guest VLAN.

Default

None

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The specified VLAN must exist as a static VLAN before configuring it as the authentication guest VLAN. This command is available for physical port interface configuration.
The host cannot access the network until it passes the authentication. If the guest VLAN is configured, the host is allowed to access the guest VLAN without passing authentication.

During authentication, if the RADIUS server assigns a VLAN to the user, the user will be authorized to this assigned VLAN.
Guest VLAN and VLAN assignment do not take effect on trunk VLAN ports and VLAN tunnel ports.
Normally, guest VLAN and VLAN assignment are functioning for hosts that send untagged packets. It may cause unexpected behavior if it is functioning on hosts that send tagged packets.
For port-based 802.1X, the port will be added as the guest VLAN member port and PVID of the port will change to guest VLAN. Traffic that comes from guest VLAN can be forwarded regardless of whether it was authenticated. Traffic that comes from other VLANs is dropped until it passes authentication.
When one host passes authentication, the port will leave the guest VLAN and be added to the assigned VLAN. The PVID of the port will be changed to the assigned VLAN.
For MAC-based 802.1X and MAC authentication authentication; the port will be added as a guest VLAN member port and the PVID of the port will change to the guest VLAN. Hosts that are allowed to access the guest VLAN, are forbidden to access other VLANs until they pass authentication.
When one host passes authentication, the port will stay in the guest VLAN and the PVID of the port will not be changed.
If the guest VLAN is disabled, the port will leave the guest VLAN, return to the native VLAN, and the PVID will change to the native VLAN.

Example

This example shows how to configure VLAN 5 as the authentication guest VLAN.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#authentication guest-vlan 5
GA-MLxxTPoE+(config-if)#
```

11.5.5 authentication step-auth

This command is used to configure the 2-step authentication mode for the specific interface. Use the **no** form of this command clear the 2-step authentication mode for the specific interface.

Syntax

- **authentication step-auth {mac-web | mac-dot1x | dot1x-web} interface** *INTERFACE-ID* **[, | -]**
- **no authentication step-auth {mac-web | mac-dot1x | dot1x-web} interface** *INTERFACE-ID* **[, | -]**

Parameters

Parameters	Description
mac-web	Specifies to first use MAC authentication and then web authentication in the 2-step authentication mode.
mac-dot1x	Specifies to first use MAC authentication and then 802.1X authentication in the 2-step authentication mode.
dot1x-web	Specifies to first use 802.1X authentication and then web authentication in the 2-step authentication mode.
INTERFACE-ID	Specifies the interfaces to be used.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to configure the 2-step authentication mode for the specified interface. The **mac-web**, **mac-dot1x**, and **dot1x-web** options can be configured on the same interface at the same time. 2-step authentication will allow access to clients where two authentication methods succeeded.
If **MAC authentication** is used as the first step, the **MAC authentication account** is required to include the following attribute to specify the second authentication method:

- *RADIUS: Filter-ID = "AUTH-WEB"* - This is required for Web authentication as the second step.
- *RADIUS: Filter-ID = "AUTH-802.1X"* - This is required for 802.1X authentication as the second step.
- *RADIUS: Filter-ID = "AUTH-ANY"* - This is required for Web or 802.1X authentication as the second step.

When no Filter-ID exists, the DUT will treat the configuration as single MAC authentication.
In the local database, the "2-step authentication Status" field will be:

- **802.1X** - When 802.1X authentication is required as the second step.
- **WEB** - When Web authentication is required as the second step.
- **Any** - When Web or 802.1X authentication is required as the second step.
- **No** - When the second step for authentication is not defined (single MAC authentication).

The following command can be used to specify the "2-step authentication Status" for local MAC authentication:

- **aaa authentication auth-mac** *MAC-ADDRESS* **vlan** *VLAN-ID* **filter-id** *NUMBER* **step-auth {no | dot1x | web | any}**

If **802.1X authentication** is used as the first step, the **802.1X authentication account** is required to include the following attribute to specify the second authentication method:

- ***RADIUS: Filter-ID = "AUTH-WEB"*** - This is required for Web authentication as the second step.

When no Filter-ID exists, the DUT will treat the configuration as single 802.1X authentication.
In the local database, the "2-step authentication Status" field will be:

- **Enabled** - When Web authentication is required as the second step.
- **Disabled** - When the second step for authentication is not defined (single 802.1X authentication).

The following command can be used to specify the "2-step authentication Status" for local 802.1X authentication:

- **aaa authentication auth-user** *STRING* **{password** *STRING* **[encrypt] | encrypt-password** *STRING***} vlan** *VLAN-ID* **filter-id** *NUMBER* **auth-type {both | web | dot1x} step-auth {enable | disable}**

If the second step for authentication (configured using the abovementioned command) and the second step for authentication in the port settings (MAC-WEB Auth Ports, MAC-802.1X Auth Ports, and 802.1X-WEB Auth Ports) are different, then authentication will be rejected.

Example

This example shows how to configure to use MAC and web authentication as the 2-step authentication mode on Gigabit Ethernet 1/0/1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#authentication step-auth mac-web interface gi1/0/1
GA-MLxxTPoE+(config)#
```

11.5.6 authentication step-auth second-step-timeout

This command is used to configure the timeout value for the first authentication success module.

Syntax

- **authentication step-auth second-step-timeout** *SECONDS*

Parameters

Parameters	Description
SECONDS	Specifies the timeout value in seconds for the first authentication success module. The value is from 0-65535.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to configure the timeout value for the first authentication success module. If the first authentication succeeded but not the second authentication, the first authentication will be rejected after the timeout.

Example

This example shows how to configure the timeout value of 2-step authorization.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#authentication step-auth second-step-timeout 200
GA-MLxxTPoE+(config)#
```

11.5.7 no authentication mac

This command is used to remove authentication sessions.

Syntax

- no authentication mac *MAC-ADDRESS*

Parameters

Parameters	Description
MAC-ADDRESS	Specifies MAC address to clear authentication sessions.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to remove authentication sessions.

Example

This example shows how to remove authentication sessions.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#no authentication mac 00-40-10-28-19-78
GA-MLxxTPoE+(config)#
```

11.5.8 show authentication

This command is used to display the authentication settings.

Syntax

- show authentication

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to display the authentication settings.

Example

This example shows how to display the authentication settings.

```
GA-MLxxTPoE+#show authentication

 Global MAC Auth Status : Disabled        Global WEB Auth Status : Disabled

 802.1X Port-based Auth Ports :1/0/1-1/0/30
 802.1X MAC-based Auth Ports  :
 MAC Auth Ports               :
 WEB Auth Ports               :
 Syslog Transmission          :Enabled

GA-MLxxTPoE+#
```

11.5.9 show authentication dynamic-vlan

This command is used to display the dynamic VLAN information of authentication.

Syntax

- **show authentication dynamic-vlan**

Parameters

None

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to display the dynamic VLAN information of authentication.

Example

This example shows how to display the dynamic VLAN information of authentication.

```
GA-MLxxTPoE+#show authentication dynamic-vlan

 Accept RADIUS Attribute: Enabled

 Port      Current PVID Auth Status  Guest  Default
 --------- ------------ ------------ ------ -------
   Gi1/0/1            1   Authorized   ----    ----
   Gi1/0/2            1   Authorized   ----    ----
   Gi1/0/3            1   Authorized   ----    ----
   Gi1/0/4            1   Authorized   ----    ----
   Gi1/0/5            1   Authorized   ----    ----
   Gi1/0/6            1   Authorized   ----    ----
   Gi1/0/7            1   Authorized   ----    ----
   Gi1/0/8            1   Authorized   ----    ----
   Gi1/0/9            1   Authorized   ----    ----
  Gi1/0/10            1   Authorized   ----    ----
  Gi1/0/11            1   Authorized   ----    ----
  Gi1/0/12            1   Authorized   ----    ----
  Gi1/0/13            1   Authorized   ----    ----
  Gi1/0/14            1   Authorized   ----    ----
  Gi1/0/15            1   Authorized   ----    ----
  Gi1/0/16            1   Authorized   ----    ----
  Gi1/0/17            1   Authorized   ----    ----
  Gi1/0/18            1   Authorized   ----    ----
  Gi1/0/19            1   Authorized   ----    ----
--More--
```

11.5.10show authentication sort

This command is used to display authentication information.

Syntax

- **show authentication sort {mac | interface** *INTERFACE-ID* **[, | -]}**

Parameters

Parameters	Description
mac	Specifies to display all authentication information.
INTERFACE-ID	Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to display authentication information.

Example

This example shows how to display authentication information.

```
GA-MLxxTPoE+#show authentication sort mac

Total Hosts      :17
Authorized Hosts :2
Auth Aging Time  :1440 minutes


MAC Address       Port      Auth Type       Auth Status     Remaining Aging Time
----------------- --------- --------------- --------------- --------------------
00-01-01-01-01-01 Gi1/0/21  MAC             Authorized      1440
00-05-5D-A5-41-BF Gi1/0/21  802.1X/MAC      Unauthorized    ---
00-19-5B-E9-5C-A7 Gi1/0/24  802.1X          Authorized      ---
00-1A-4D-2A-09-20 Gi1/0/21  802.1X/MAC      Unauthorized    ---
00-1B-21-44-C6-21 Gi1/0/21  802.1X/MAC      Unauthorized    ---
00-1C-F0-C3-D4-F9 Gi1/0/21  802.1X/MAC      Unauthorized    ---
00-1D-7D-44-96-0E Gi1/0/21  802.1X/MAC      Unauthorized    ---
00-21-91-A9-3D-01 Gi1/0/21  802.1X/MAC      Unauthorized    ---
00-21-91-A9-F3-01 Gi1/0/21  802.1X/MAC      Unauthorized    ---
00-24-1D-36-E8-1B Gi1/0/21  802.1X/MAC      Unauthorized    ---
00-24-1D-EC-84-DD Gi1/0/21  802.1X/MAC      Unauthorized    ---
00-50-BA-19-59-81 Gi1/0/21  802.1X/MAC      Unauthorized    ---
00-A0-C9-E5-34-60 Gi1/0/21  802.1X/MAC      Unauthorized    ---
50-46-5D-A2-02-31 Gi1/0/21  802.1X/MAC      Unauthorized    ---
6C-F0-49-62-CA-44 Gi1/0/21  802.1X/MAC      Unauthorized    ---
6C-F0-49-C6-52-C0 Gi1/0/21  802.1X/MAC      Unauthorized    ---
74-27-EA-F1-52-9A Gi1/0/21  802.1X/MAC      Unauthorized    ---

GA-MLxxTPoE+#
```

11.6 Secure Sockets Layer (SSL)

11.6.1 no certificate

This command is used to delete the imported certificate.

Syntax

- **no certificate** *NAME*

Parameters

Parameters	Description
NAME	Specifies the name of the certificate to be deleted.

Default

None

Command Mode

Certificate Chain Configuration Mode

Command Default Level

Level: 15

Usage Guideline

Use the **show crypto pki trustpoints** command to get a name list of imported certificates. Then use this command to delete the imported certificates of a trust point. If the specified certificate is a local certificate the corresponding private key will be deleted at the same time.

Example

This example shows how to delete an imported certificate named *tongken.ca* of the trust point *gaa*.

```
GA-MLxxTPoE+# show crypto pki trustpoints

Trustpoint Name        : gaa (primary)
  Imported certificates:
    CA                 : tongken.ca
    local certificate  : webserver.crt
    local private key  : webserver.prv

GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# crypto pki certificate chain gaa
GA-MLxxTPoE+(config-cert-chain)# no certificate tongken.ca
GA-MLxxTPoE+(config-cert-chain)#
```

11.6.2 crypto pki import pem

This command is used to import the CA certificate or the Switch certificate and keys to a trust-point from privacy-enhanced mail (PEM)-formatted files.

Syntax

- **crypto pki import** *TRUSTPOINT* **pem** *FILE-SYSTEM*:/[*DIRECTORY*/]*FILE-NAME* [**password** *PASSWORD-PHRASE*] {**ca** | **local** | **both**}
- **crypto pki import** *TRUSTPOINT* **pem tftp://***IP-ADDRESS*/[*DIRECTORY*/]*FILE-NAME* [**password** *PASSWORD-PHRASE*] {**ca** | **local** | **both**}

Parameters

Parameters	Description
TRUSTPOINT	Specifies the name of the trust-point that is associated with the imported certificates and key pairs.
FILE-SYSTEM	Specifies the file system for certificates and key pairs. A colon (:) is required after the specified file system.
DIRECTORY	(Optional) Specifies the directory name where the Switch should import the certificates and key pairs in the Switch or TFTP server.
FILE-NAME	Specifies the name of the certificates and key pairs to be imported. By default, the Switch will append this name with *.ca*, *.prv* and *.crt* for CA certificate, private key and certificate respectively.
password *PASSWORD-PHRASE*	(Optional) Specifies the encrypted password phrase that is used to undo encryption when the private keys are imported. The password phrase is a string of up to 64 characters. If the password phrase is not specified, the NULL string will be used.
tftp	Specifies the source URL for a TFTP network server.
IP-ADDRESS	Specifies the IP address of the TFTP server.

Parameters	Description
ca	Specifies to import the CA certificate only.
local	Specifies to import local certificate and key pairs only.
both	Specifies to import the CA certificate, local certificate and key pairs.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 15

Usage Guideline

This command allows administrators to import certificates and key pairs in the PEM-formatted files.
Proper certificates and key pairs need to be imported to the Switch according to the desired key exchange algorithm. RSA and DSA certificates/key pairs should be imported for RSA and DHS-DSS respectively. RSA and DSA certificates and keys are incompatible. An SSL client that has only an RSA certificate and key cannot establish a connection with an SSL server that has only a DSA certificate and key.
The imported certificate(s) may form a certificate chain which establishes a sequence of trusted certificates from a peer certificate to the root CA certificate. The trust point CA is the certificate authority configured on the Switch as the trusted CA. Any obtained peer certificate will be accepted if it is signed by a locally trusted CA or its subordinates.
If the specified trust point doesn't exist, an error message will be prompted.

Example

This example shows how to import certificates (CA and local) and key pair files to trust-point "TP1" via TFTP.

```
GA-MLxxTPoE+# crypto pki import TP1 pem tftp://10.1.1.2/name/msca password abcd1234
both

% Importing CA certificate...
Destination filename [name/msca.ca]?
Reading file from tftp://10.1.1.2/name/msca.ca
Loading name/msca.ca from 10.1.1.2 (via Gi1/0/5):!
[OK - 1082 bytes]

% Importing private key PEM file...
Reading file from tftp://10.1.1.2/name/msca.prv
Loading name/msca.prv from 10.1.1.2 (via Gi1/0/5):!
[OK - 573 bytes]

% Importing certificate PEM file...
Reading file from tftp://10.1.1.2/name/msca.crt
Loading name/msca.crt from 10.1.1.2 (via Gi1/0/5):!
[OK - 1289 bytes]
% PEM files import succeeded.

GA-MLxxTPoE+(config)#
```

11.6.3 crypto pki trustpoint

This command is used to declare the trust-point that the Switch will use. Use the **no** form of this command to delete all certificates and key pairs associated with the trust-point.

Syntax

- **crypto pki trustpoint** *NAME*
- **no crypto pki trustpoint** *NAME*

Parameters

Parameters	Description
NAME	Specifies to create a name for the trust-point.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to declare a trust-point, which can be a self-signed root certificate authority (CA) or a subordinate CA. Issuing this command will enter the CA-Trust-Point Configuration Mode.

Example

This example shows how to declare a trust-point "TP1" and specify it is a primary trust-point.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# crypto pki trustpoint TP1
GA-MLxxTPoE+(ca-trustpoint)# primary
GA-MLxxTPoE+(ca-trustpoint)#
```

11.6.4 crypto pki certificate chain

This command is used to enter into the certificate chain configuration mode.

Syntax

- **crypto pki certificate chain** *NAME*

Parameters

Parameters	Description
NAME	Specifies the name for the trust-point.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

Use this command to enter into certificate chain configuration mode. If the specified trust-point name doesn’t exist, an error message will be displayed.

Example

This example shows how to enter into certificate chain configuration mode.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# crypto pki certificate chain TP1
GA-MLxxTPoE+(trustpoint)#
```

11.6.5 primary

This command is used to assign a specified trust-point as the primary trust-point of the Switch. Use the **no** form of this command to disable the option.

Syntax

- **primary**
- **no primary**

Parameters

None

Default

By default, this option is disabled.

Command Mode

CA-Trust-Point Configuration Mode

Command Default Level

Level: 15

Usage Guideline

Use the primary command to specify a given trust-point as primary. This trust-point can be used as default trust-point when the application doesn't explicitly specify which certificate authority (CA) trust-point should be used. Only one trust-point can be specified as the primary. The last trust-point specified as the primary will overwrite the previous one.

Example

This example shows how to configure the trust-point “TP1” as the primary trust-point.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# crypto pki trustpoint TP1
GA-MLxxTPoE+(ca-trustpoint)# primary
GA-MLxxTPoE+(ca-trustpoint)#
```

11.6.6 show crypto pki trustpoints

This command is used to display the trust-points that are configured in the Switch.

Syntax

- **show crypto pki trustpoints** [*TRUSTPOINT*]

Parameters

Parameters	Description
TRUSTPOINT	(Optional) Specifies the name of the trust-point to be displayed.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

If no parameter is specified, all trust-points will be displayed.

Example

This example shows how to display all trust-points.

```
GA-MLxxTPoE+# show crypto pki trustpoints

Trustpoint Name        : TP1 (primary)
  Imported certificates:
    CA                 : tongken.ca
    local certificate  : webserver.crt
    local private key  : webserver.prv

Trustpoint Name        : TP2
  Imported certificates:
    CA                 : chunagtel.ca
    local certificate  : openflow.crt
    local private key  : openflow.prv

GA-MLxxTPoE+#
```

11.6.7 show ssl-service-policy

This command is used to display the SSL service policy.

Syntax

- **show ssl-service-policy** [*POLICY-NAME*]

Parameters

Parameters	Description
POLICY-NAME	(Optional) Specifies the name of the SSL service policy.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

When the name of the SSL service policy is not specified, all SSL service policies will be displayed.

Example

This example shows how to display all SSL service policies.

```
GA-MLxxTPoE+# show ssl-service-policy

SSL Policy Name        : ssl-server
  Enabled Versions     :
    TLS 1.0
    TLS 1.1
    TLS 1.2
  Enabled CipherSuites :
    RSA_WITH_AES_128_CBC_SHA,
    RSA_WITH_AES_256_CBC_SHA,
    RSA_WITH_AES_128_CBC_SHA256,
    RSA_WITH_AES_256_CBC_SHA256,
    DHE_DSS_WITH_AES_256_CBC_SHA,
    DHE_RSA_WITH_AES_256_CBC_SHA
  Session Cache Timeout: 600
  Secure Trustpoint    : TP1
GA-MLxxTPoE+#
```

11.6.8 ssl-service-policy

This command is used to configure the SSL service policy.

Syntax

- ssl-service-policy *POLICY-NAME* [version [tls1.0] [tls1.1] [tls1.2]] |[ciphersuite [rsa-aes-128-cbc-sha] [rsa-aes-256-cbc-sha] [rsa-aes-128-cbc-sha256] [rsa-aes-256-cbc-sha256] [dhe-dss-aes-256-cbc-sha] [dhe-rsa-aes-256-cbc-sha]]| secure-trustpoint *TRUSTPOINT* | session-cache-timeout *TIME-OUT*]
- no ssl-service-policy *POLICY-NAME* [version [tls1.0] [tls1.1] [tls1.2]] |[ciphersuite [rsa-aes-128-cbc-sha] [rsa-aes-256-cbc-sha] [rsa-aes-128-cbc-sha256] [rsa-aes-256-cbc-sha256] [dhe-dss-aes-256-cbc-sha] [dhe-rsa-aes-256-cbc-sha]]| secure-trustpoint | session-cache-timeout]

Parameters

Parameters	Description
POLICY-NAME	Specifies the name of the SSL service policy.
version	(Optional) Specifies the TLS version. **tls1.0** - Indicate the applicance accepts TLS version 1.0. **tls1.1** - Indicate the applicance accepts TLS version 1.1. **tls1.2** - Indicate the applicance accepts TLS version 1.2.

Parameters	Description
ciphersuite	(Optional) Specifies the cipher suites that should be used by the secure service when negotiating a connection with a remote peer. **rsa-aes-128-cbc-sha** - Use RSA key exchange with AES 128-bit encryption for message encryption and SHA for message digest. **rsa-aes-256-cbc-sha** - Use RSA key exchange with AES 256-bit encryption for message encryption and SHA for message digest. **rsa-aes-128-cbc-sha256** - Use RSA key exchange with AES 128-bit encryption for message encryption and SHA 256 bits for message digest. **rsa-aes-256-cbc-sha256** - Use RSA key exchange with AES 256-bit encryption for message encryption and SHA 256 bits for message digest. **dhe-dss-aes-256-cbc-sha** - Use DH key exchange with AES 256-bit encryption for message encryption and SHA for message digest. **dhe-rsa-aes-256-cbc-sha** - Use DH key exchange with AES 256-bit encryption for message encryption and SHA for message digest. When the cipher suite is not configured, the SSL client and server will negotiate the best cipher suite that they both support from the list of available cipher suites. Multiple cipher suites can be specified to be used. Use the **no** form of this command to disable the selected cipher suites.
secure-trustpoint *TRUSTPOINT*	(Optional) Specifies the name of the trust-point that should be used in SSL handshake. When this parameter is not specified, the trust-point which is specified as the primary will be used. If no primary trust-point is specified, the built-in certificate/key pairs will be used. Use the **no** form of this command to cancel the specified trust-point and use the built-in certificate/key pairs.
session-cache-timeout *TIME-OUT*	(Optional) Specifies the timeout value in seconds for the information stored in the SSL session cache. The valid range is from 60 to 86400. When this parameter is not configured, the default session cache timeout is 600 seconds Use the **no** form of this command to revert the SSL session cache timeout to the default setting.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 15

Usage Guideline

This command is used to configure the SSL service policy.

Example

This example shows how to configure the SSL service policy “ssl-server” which associates the “TP1” trust-point.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# ssl-service-policy ssl-server secure-trustpoint TP1
GA-MLxxTPoE+(config)#
```

12 Redundancy Function

12.1 STP (Spanning Tree Protocol) Commands

STP

STP (Spanning Tree Protocol) is a function to provide path redundancy while preventing loops in a network established by connecting multiple bridges. Even if one end of a communication route is down, the function can continue communications by detouring the route.
In general, if a cable is connected in a loop form, a phenomenon called broadcast storm, where frames keep looping permanently, occurs and causes the network to go down.
The SPT function interchanges control frames called BPDU frames between switches to calculate the shortest route. Automatic port blocking to prevent frames from looping allows you to establish a network which logically has no loops.
If a failure occurs on a route, the communication route can be recovered within 50 seconds or less.

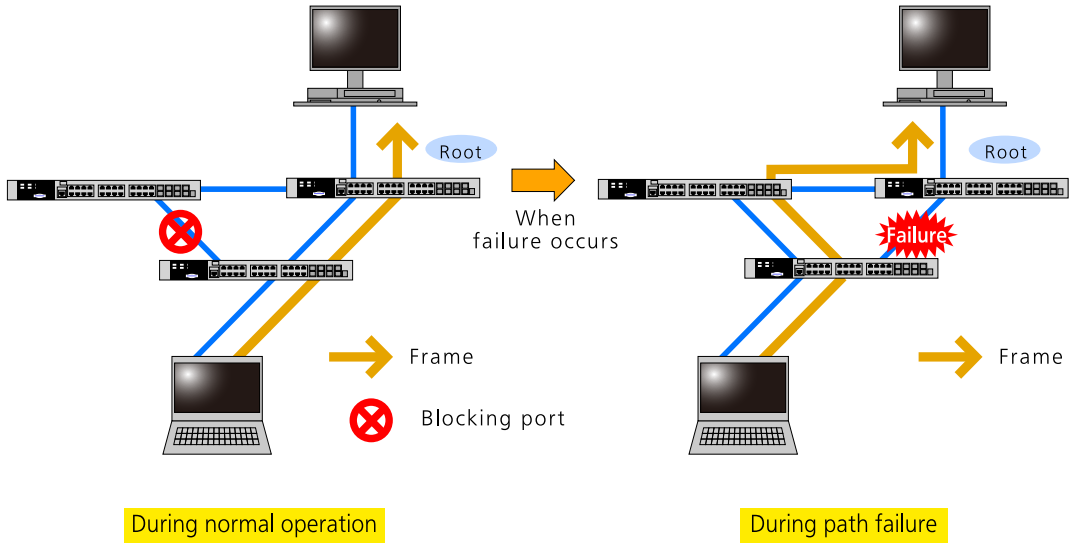


Figure 71-1 STP overview

RSTP

RSTP (Rapid Spanning Tree Protocol) is a modified STP protocol to reduce recovery time to several seconds during a route failure.

When changing a route, the RSTP function determines port roles and changes the route immediately through information exchanges (proposal/agreement) between switches instead of timers used in STP.

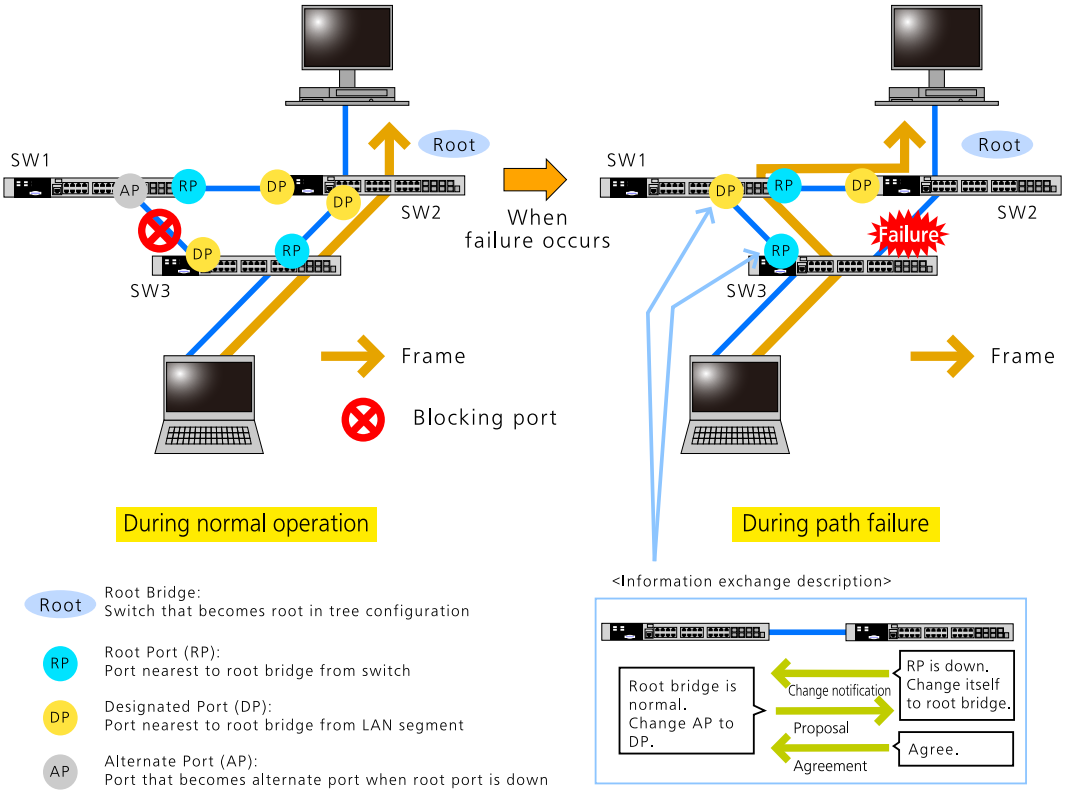


Figure 71-2 RSTP overview

MSTP

MSTP (Multiple Spanning Tree Protocol) is also a modified STP protocol to communicate data for each VLAN using different routes. This allows for effective use of bandwidth.
Consolidating multiple VLANS into a group called instance can reduce more CPU loads compared to when designing a spanning tree instance for each VLAN.
The MSTP function allows for supporting a large-size network.

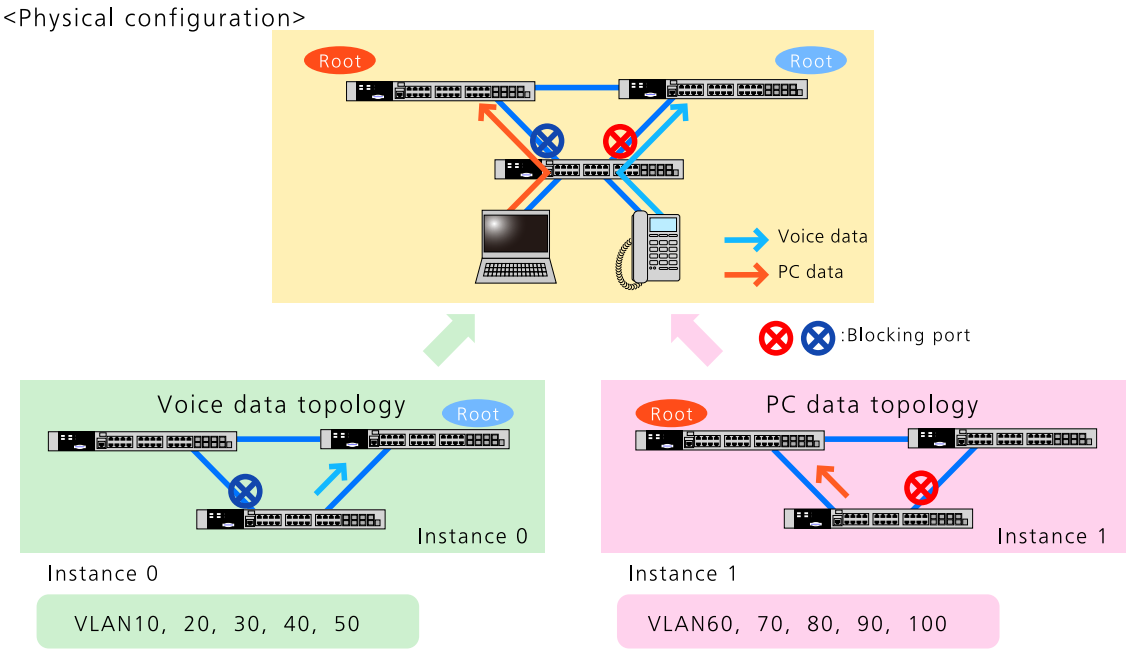


Figure 71-3 MSTP overview

12.1.1 clear spanning-tree detected-protocols

This command is used to restart the protocol migration.

Syntax

- **clear spanning-tree detected-protocols {all | interface** *INTERFACE-ID*}

Parameters

Parameters	Description
all	Specifies to trigger the detection action for all ports.
interface *INTERFACE-ID*	Specifies the port interface that will be triggered the detecting action.

Default

None

Command Mode

Privileged EXEC Mode

Command Default Level

Level: 12

Usage Guideline

Using this command the port protocol migrating state machine will be forced to the *SEND_RSTP* state. This action can be used to test whether all legacy bridges on a given LAN have been removed. If there is no STP Bridge on the LAN, the port will be operated in the configured mode, either in the RSTP or MSTP mode. Otherwise, the port will be operated in the STP mode.

Example

This example shows how to trigger the protocol migration event for all ports.

```
GA-MLxxTPoE+# clear spanning-tree detected-protocols all
GA-MLxxTPoE+#
```

12.1.2 show spanning-tree

This command is used to display the information of spanning tree protocol operation. This command is only for STP and RSTP.

Syntax

- **show spanning-tree [interface [***INTERFACE-ID* **[, | -]]**

Parameters

Parameters	Description
interface *INTERFACE-ID*	(Optional) Specifies the interface ID to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display the Spanning Tree configuration for the single spanning tree when in the RSTP or STP-compatible mode.

Example

This example shows how to display the spanning tree information when STP is enabled.

```
GA-MLxxTPoE+#show spanning-tree

 Spanning Tree      : Enabled
 Protocol Mode      : RSTP
 Tx-hold-count      : 6
 Root ID Priority   : 32768
         Address    : 00-50-40-xx-xx-xx
         Hello Time : 2 sec  Max Age : 20 sec  Forward Delay : 15 sec
 Bridge ID Priority : 32768 (priority 32768  sys-id-ext 0)
         Address    : 00-50-40-xx-xx-xx
         Hello Time : 2 sec  Max Age : 20 sec  Forward Delay : 15 sec
 Topology Changes Count : 0

                                                 Priority Link
 Interface      Role       State      Cost       .Port#   Type   Edge
 ---------      ----       -----      ----       -------  -----  ----
 Gi1/0/6        designated forwarding 20000      128.6    p2p    edge


GA-MLxxTPoE+#
```

12.1.3 show spanning-tree mst

This command is used to display the information of Multiple Spanning Tree (MST) and instances.

Syntax

- **show spanning-tree mst {configuration | instance** *INTANCE-ID* **[interface** *INTERFACE-ID***]}**

Parameters

Parameters	Description
configuration	Specifies the MST configuration of the equipment.
instance *INTANCE-ID*	Specifies the instance number.

Parameters	Description
interface *INTERFACE-ID*	Specifies the interface ID to be displayed.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display MST information.

Example

This example shows how to display spanning tree configuration information for GigabitEthernet1/0/1.

```
GA-MLxxTPoE+#show spanning-tree mst

 Spanning tree           : Enabled
 Protocol                : RSTP
 Number of MST Instances : 1

 >>>>MST00  VLANs mapped   : 1-4094
 Bridge Address            : 00-50-40-xx-xx-xx  Priority : 32768 (32768 sysid 0)
 Designated Root Address   : 00-50-40-xx-xx-xx  Priority : 32768 (32768 sysid 0)
 CIST External Root Cost   : 0
 Regional Root Address     : 00-50-40-xx-xx-xx  Priority : 32768 (32768 sysid 0)
 CIST Internal Root Cost   : 0
 Designated Bridge Address : 00-50-40-xx-xx-xx  Priority : 32768 (32768 sysid 0)
 Topology Changes Count    : 0

                                                Priority Link
 Interface      Role       State      Cost      .Port#   Type   Edge
 ---------      ----       -----      ----      -------  -----  ----
 Gi1/0/6        designated forwarding 20000     128.6    p2p    edge


GA-MLxxTPoE+#
```

12.1.4 show spanning-tree configuration interface

This command is used to display the information about STP interface related configuration.

Syntax

- show spanning-tree configuration interface [*INTERFACE-ID* [, | -]]

Parameters

Parameters	Description
INTERFACE-ID	(Optional) Specifies the interface ID to be displayed.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of interfaces. No space before and after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display Spanning Tree interface level configuration. The command can be used for all STP versions.

Example

This example shows how to display spanning tree configuration information for GigabitEthernet1/0/1.

```
GA-MLxxTPoE+#show spanning-tree configuration interface GigabitEthernet 1/0/1

Gi1/0/1
 Spanning tree state : Enabled
 Port path cost: 0
 Port priority: 128
 Port Identifier:  128.1
 Link type: auto
 Port Fast: edge
 Hello Time          : 2
 Guard Root          : Disabled
 TCN Filter          : Disabled
 BPDU Forward        : Disabled

GA-MLxxTPoE+#
```

12.1.5 spanning-tree global state

This command is used to enable or disable the STP's global state. Use the **no** form of this command to disable the STP's global state.

Syntax

- **spanning-tree global state {enable | disable}**
- **no spanning-tree global state**

Parameters

Parameters	Description
enable	Specifies to enable the STP's global state.
disable	Specifies to disable the STP's global state.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command in the global configuration mode to enable the global spanning-tree function.

Example

This example shows how to enable the spanning-tree function.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# spanning-tree global state enable
GA-MLxxTPoE+(config)#
```

12.1.6 spanning-tree (timers)

This command is used to configure the Spanning Tree timer value. Use the **no** form of this command to revert to the default settings.

Syntax

- **spanning-tree** {**hello-time** *SECONDS* | **forward-time** *SECONDS* | **max-age** *SECONDS*}
- **no spanning-tree** {**hello-time** | **forward-time** | **max-age**}

Parameters

Parameters	Description
hello-time *SECONDS*	Specifies the interval that a designated port will wait between the periodic transmissions of each configuration message. The range is from 1 to 2 seconds.
forward-time *SECONDS*	Specifies the forward delay time used by STP to transition from the listening to the learning states and learning to forwarding states. The range is from 4 to 30 seconds.
max-age *SECONDS*	Specifies the maximum message age of BPDU. The range is from 6 to 40 seconds.

Default

The default value of the hello-time is 2 seconds.
The default value of the forward-time is 15 seconds.
The default value of the max-age is 20 seconds.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to configure the Spanning Tree timer value.

Example

This example shows how to configure the STP timers.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# spanning-tree hello-time 1
GA-MLxxTPoE+(config)# spanning-tree forward-time 16
GA-MLxxTPoE+(config)# spanning-tree max-age 21
GA-MLxxTPoE+(config)#
```

12.1.7 spanning-tree state

This command is used to enable or disable the STP operation. Use the **no** form of this command to revert to the default setting.

Syntax

- **spanning-tree state {enable | disable}**
- **no spanning-tree state**

Parameters

Parameters	Description
enable	Specifies to enable STP for the configured interface.
disable	Specifies to disable STP for the configured interface.

Default

By default, this option is enabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

When a port is spanning tree enabled, the spanning tree protocol engine will either send or process the spanning tree BPDU received by the port. The command should be used with caution to prevent bridging loops. The command does not take effect if the Layer 2 protocol tunnel is enabled for STP.

Example

This example shows how to enable Spanning Tree on GigabitEthernet1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# spanning-tree state enable
GA-MLxxTPoE+(config-if)#
```

12.1.8 spanning-tree cost

This command is used to configure the value of the port path-cost on the specified port. Use the **no** form of this command to the auto-computed path cost.

Syntax

- **spanning-tree cost** *COST*
- **no spanning-tree cost**

Parameters

Parameters	Description
COST	Specifies the path cost for the port. The range is from 1 to 200000000.

Default

The default path cost is computed from the interface's bandwidth setting.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

In the RSTP or STP-compatible mode, the administrative path cost is used by the single spanning-tree to accumulate the path cost to reach the Root. In the MSTP mode, the administrative path cost is used by the CIST regional root to accumulate the path cost to reach the CIST root.

Example

This example shows how to configure the port cost to 20000 for GigabitEthernet1/0/7.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/7
GA-MLxxTPoE+(config-if)# spanning-tree cost 20000
GA-MLxxTPoE+(config-if)#
```

12.1.9 spanning-tree guard root

This command is used to enable the root guard mode. Use the **no** form of this command to revert to the default setting.

Syntax

- **spanning-tree guard root**
- **no spanning-tree guard root**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

BPDU guard prevents a port from becoming a root port. This feature is useful for the service provider to prevent external bridges to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator.
When a port is guarded from becoming a root port, the port will only play the role as a designated port. If the port receives the configuration BPDU with a higher priority, the port will change to the alternate port, which is in the blocking state. The received superior factor will not participate in the STP computation. The port will listen for BPDUs on the link. If the port times out the received superior BPDU, it will change to the designated port role.
When a port changes to the alternate port state, due to the root guard, a system message will be generated. This configuration will take effect for all the spanning-tree versions.

Example

This example shows how to configure to prevent interface GigabitEthernet1/0/1 from being a root port.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# spanning-tree guard root
GA-MLxxTPoE+(config-if)#
```

12.1.10spanning-tree link-type

This command is used to configure a link-type for a port. Use the **no** form of this command to revert to the default setting.

Syntax

- **spanning-tree link-type {point-to-point | shared}**
- **no spanning-tree link-type**

Parameters

Parameters	Description
point-to-point	Specifies that the port's link type is point-to-point.
shared	Specifies that the port's link type is a shared media connection.

Default

The link type is automatically derived from the duplex setting unless explicitly configuring the link type.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

A full-duplex port is considered to have a point-to-point connection; on the opposite, a half-duplex port is considered to have a shared connection. The port can't transit into forwarding state rapidly by setting link type to shared-media. Hence, auto-determined of link-type by the STP module is recommended.
This configuration will take effect for all the spanning-tree modes.

Example

This example shows how to configure the link type to point-to-point for port GigabitEthernet1/0/7.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/7
GA-MLxxTPoE+(config-if)# spanning-tree link-type point-to-point
GA-MLxxTPoE+(config-if)#
```

12.1.11spanning-tree mode

This command is used to configure the STP mode. Use the **no** form of this command to revert to the default setting.

Syntax

- **spanning-tree mode {mstp | rstp |stp}**
- **no spanning-tree mode**

Parameters

Parameters	Description
mstp	Specifies the Multiple Spanning Tree Protocol (MSTP).

Parameters	Description
rstp	Specifies the Rapid Spanning Tree Protocol (RSTP).
stp	Specifies the Spanning Tree Protocol (IEEE 802.1D Compatible)

Default

By default, this mode is RSTP.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

If the mode is configured as STP or RSTP, all currently running MSTP instances will be cancelled automatically. If the newly configured mode is changed from the previous one, the spanning-tree state machine will restart again, therefore all of the stable spanning-tree port states will transit into discarding states.

Example

This example shows how to configure the running version of the STP module to RSTP.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# spanning-tree mode rstp
GA-MLxxTPoE+(config)#
```

12.1.12spanning-tree portfast

This command is used to specify the port's fast mode. Use the **no** form of this command to revert to the default setting.

Syntax

- **spanning-tree portfast {disable | edge| network}**
- **no spanning-tree portfast**

Parameters

Parameters	Description
disable	Specifies to set the port to the port fast disabled mode.
edge	Specifies to set the port to the port fast edge mode.
network	Specifies to set the port to the port fast network mode.

Default

By default, this option is **edge**.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

A port can be in one of the following three port fast modes:

- **Edge mode -** The port will directly change to the spanning-tree forwarding state when a link-up occurs without waiting for the forward-time delay. If the interface receives a BPDU later, its operation state changes to the non-port-fast state.
- **Disable mode -** The port will always be in the non-port-fast state. It will always wait for the forward-time delay to change to forwarding state.
- **Network mode -** The port will remain in the non-port-fast state for three seconds. The port will change to the port-fast state if no BPDU is received and changes to the forwarding state. If the port received the BPDU later, it will change to the non-port-fast state

This command should be used with caution. Otherwise, an accidental topology loop and data-packet loop may be generated and disrupt the network operation.

Example

This example shows how to configure port GigabitEthernet1/0/7 to the port-fast edge mode.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/7
GA-MLxxTPoE+(config-if)# spanning-tree portfast edge
GA-MLxxTPoE+(config-if)#
```

12.1.13spanning-tree port-priority

This command is used to configure the value of the STP port priority on the specified port. It is only used for RSTP and STP versions. Use the **no** form of this command to revert to the default setting.

Syntax

- **spanning-tree port-priority** *PRIORITY*
- **no spanning-tree port-priority**

Parameters

Parameters	Description
PRIORITY	Specifies the port priority. Valid values are from 0 to 240.

Default

By default, this value is 128.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The port priority and the port number together form the Port Identifier. It will be used in the computation of the role of the port. This parameter is used only in the RSTP and STP-compatible mode. A smaller number represents a better priority.

Example

This example shows how to configure the port priority to 0 for port GigabitEthernet1/0/7.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/7
GA-MLxxTPoE+(config-if)# spanning-tree port-priority 0
GA-MLxxTPoE+(config-if)#
```

12.1.14spanning-tree priority

This command is used to configure the bridge priority. It is only used for RSTP and STP versions. Use the **no** form of this command to revert to the default setting.

Syntax

- **spanning-tree priority** *PRIORITY*
- **no spanning-tree priority**

Parameters

Parameters	Description
PRIORITY	Specifies that the bridge priority and bridge MAC address together forms the Spanning-Tree Bridge-ID, which is an important factor in the Spanning-Tree topology. The range is from 0 to 61440.

Default

By default, this value is 32768.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The bridge priority value is one of the two parameters used to select the Root Bridge. The other parameter is system's MAC address. The bridge's priority value must be divisible by 4096 and a smaller number represents a better priority. This configuration will take effect on STP version and RSTP mode. In the MSTP mode, use the command **spanning-tree mst priority** to configure the priority for an MSTP instance.

Example

This example shows how to configure the STP bridge priority value to 4096.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# spanning-tree priority 4096
GA-MLxxTPoE+(config)#
```

12.1.15spanning-tree tcnfilter

This command is used to enable Topology Change Notification (TCN) filtering at the specific interface. Use the **no** form of this command disable TCN filtering.

Syntax

- **spanning-tree tcnfilter**
- **no spanning-tree tcnfilter**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Enabling TC filtering on a port is useful for an ISP to prevent the external bridge to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator.
When a port is set to the TCN filter mode, the TC event received by the port will be ignored. This configuration will take effect for all the spanning-tree modes.

Example

This example shows how to configure TCN filtering on port GigabitEthernet1/0/7.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/7
GA-MLxxTPoE+(config-if)# spanning-tree tcnfilter
GA-MLxxTPoE+(config-if)#
```

12.1.16spanning-tree tx-hold-count

This command is used to limit the maximum number of BPDUs that can be sent before pausing for one second. Use the **no** form of this command to revert to the default setting.

Syntax

- **spanning-tree tx-hold-count** *VALUE*
- **no spanning-tree tx- hold-count**

Parameters

Parameters	Description
VALUE	Specifies the maximum number of BPDUs that can be sent before pausing for one second. The range is from 1 to 10.

Default

By default, this value is 6.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command specifies the number of hold BPDUs to transmit. The transmission of BPDUs on a port is controlled by a counter. The counter is incremented on every BPDU transmission and decremented once a second. The transmissions are paused for one second if the counter reaches the transmit hold count.

Example

This example shows how to configure the transmit hold count value to 5.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# spanning-tree tx-hold-count 5
GA-MLxxTPoE+(config)#
```

12.1.17spanning-tree forward-bpdu

This command is used to enable the forwarding of the spanning tree BPDU. Use the no form of this command to disable the forwarding of the spanning tree BPDU.

Syntax

- spanning-tree forward-bpdu
- no spanning-tree forward-bpdu

Parameters

None

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

If enabled, the received STP BPDU will be forwarded to all VLAN member ports in the untagged form. The command does not take effect if the Layer 2 protocol tunnel is enabled for STP.

Example

This example shows how to enable the forwarding of STP BPDUs.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/2
GA-MLxxTPoE+(config-if)#spanning-tree state disable
GA-MLxxTPoE+(config-if)#spanning-tree forward-bpdu
GA-MLxxTPoE+(config-if)#
```

12.2 MSTP (Multiple Spanning Tree Protocol) Commands

12.2.1 spanning-tree mst configuration

This command is used to enter the MST configuration mode and configure the MSTP region. Use the **no** form of this command to revert all settings in the MST configuration mode to the default settings.

Syntax

- **spanning-tree mst configuration**
- **no spanning-tree mst configuration**

Parameters

None

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to enter the MST configuration mode.

Example

This example shows how to enter the MST configuration mode.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#spanning-tree mst configuration
GA-MLxxTPoE+(config-mst)#
```

12.2.2 instance

This command is used to map VLANs to an MST instance. Use the **no instance** *INSTANCE-ID* command to remove the specified MST instance. Use the **no instance** *INSTANCE-ID* **vlans** *VLAND-ID* **[, | -]** command to return the VLANs to the default instance (CIST).

Syntax

- **instance** *INSTANCE-ID* **vlans** *VLAN-ID* **[, | -]**
- **no instance** *INSTANCE-ID* **[vlans** *VLAN-ID* **[, | -]]**

Parameters

Parameters	Description
INSTANCE-ID	Specifies the MSTP instance identifier that is mapped with the specified VLANs. The value is from 1 to 8.
VLAN-ID	Specifies the VLAN ID to be configured.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.

Default

By default, all VLANs are mapped with the CIST (instance 0).

Command Mode

MST Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to map VLANs to an MST instance. When mapping VLANs to a MST instance, the instance will be created automatically if the instance does not exist.

Example

This example shows how to map VLANs to an MST instance.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#spanning-tree mst configuration
GA-MLxxTPoE+(config-mst)#instance 2 vlans 1-100
GA-MLxxTPoE+(config-mst)#
```

12.2.3 name

This command is used to configure the name of an MST region. Use the **no** form of this command to revert to the default setting.

Syntax

- **name** *NAME*
- **no name**

Parameters

Parameters	Description
NAME	Specifies the name for the MST region. The maximum length is 32 characters.

Default

By default, the name is the bridge MAC address.

Command Mode

MST Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to configure the name of an MST region. When more than one switch with the same VLAN mapping and configuration version number, but with different region names, they are considered to be in different MST regions.

Example

This example shows how to configure the name of the MST region as “MSTP”.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#spanning-tree mst configuration
GA-MLxxTPoE+(config-mst)#name MSTP
GA-MLxxTPoE+(config-mst)#
```

12.2.4 revision

This command is used to configure the revision number for the MST configuration. Use the **no** form of this command to revert to the default setting.

Syntax

- **revision** *REVISION*
- **no revision**

Parameters

Parameters	Description
REVISION	Specifies the different revision level when the name is the same. The value is from 0 to 65535.

Default

By default, the value is 0.

Command Mode

MST Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to configure the revision number for the MST configuration. When more than one switch with the same configuration but different revision numbers, they are considered to be in different MST regions.

Example

This example shows how to configure the revision number for the MST configuration to “2”.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#spanning-tree mst configuration
GA-MLxxTPoE+(config-mst)#revision 2
GA-MLxxTPoE+(config-mst)#
```

12.2.5 spanning-tree mst

This command is used to configure the path cost and port priority for the MST instance. Use the **no** form of this command to revert to the default settings.

Syntax

- **spanning-tree mst** *INSTANCE-ID* {**cost** *COST* | **port-priority** *PRIORITY*}
- **no spanning-tree mst** *INSTANCE-ID* {**cost** | **port-priority**}

Parameters

Parameters	Description
INSTANCE-ID	Specifies the MSTP instance identifier. The value is from 0 to 64. The value 0 represents the default instance, CIST.
cost *COST*	Specifies the path cost of the instance. The value is from 0 to 200000000.
port-priority *PRIORITY*	Specifies the port priority of the instance. The value is from 0 to 240 in increments of 16.

Default

The cost is defined based on the port speed. The faster the speed is, the smaller cost value it is. MST always uses long path cost.
The port priority is 128.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is only available for the physical ports.

Example

This example shows how to configure the interface path cost.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/3
GA-MLxxTPoE+(config-if)#spanning-tree mst 0 cost 17031970
GA-MLxxTPoE+(config-if)#
```

This example shows how to configure the port priority.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#interface gi1/0/3
GA-MLxxTPoE+(config-if)#spanning-tree mst 0 port-priority 64
GA-MLxxTPoE+(config-if)#
```

12.2.6 spanning-tree mst max-hops

This command is used to configure the MSTP maximum hop count. Use the **no** form of this command to revert to the default setting.

Syntax

- **spanning-tree mst max-hops** *HOP-COUNT*
- **no spanning-tree mst max-hops**

Parameters

Parameters	Description
HOP-COUNT	Specifies the MSTP maximum hop count. The value is from 1 to 40.

Default

By default the MSTP maximum hop count is 20.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to configure the MSTP maximum hop count.

Example

This example shows how to configure the MSTP maximum hop count.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#spanning-tree mst max-hops 19
GA-MLxxTPoE+(config)#
```

12.2.7 spanning-tree mst hello-time

This command is used to configure the hello time used in MSTP version for each port. Use the **no** form of this command to revert to the default setting.

Syntax

- **spanning-tree mst hello-time** *SECONDS*
- **no spanning-tree mst hello-time**

Parameters

Parameters	Description
SECONDS	Specifies the interval of sending one BPDU at the designated port. The range is from 1 to 2 seconds.

Default

By default, the hello-time is 2 seconds.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

This command is used to configure the hello time used in MSTP version for each port. This only takes effects in the MSTP mode.

Example

This example shows how to configure the hello time used in MSTP version for gi1/0/1.

```
GA-MLxxTPoE+(config)#interface gi1/0/1
GA-MLxxTPoE+(config-if)#spanning-tree mst hello-time 1
GA-MLxxTPoE+(config-if)#
```

12.2.8 spanning-tree mst priority

This command is used to configure the bridge priority for the specified MSTP. Use the **no** form of this command to revert to the default setting.

Syntax

- **spanning-tree mst** *INSTANCE-ID* **priority** *PRIORITY*
- **no spanning-tree mst** *INSTANCE-ID* **priority**

Parameters

Parameters	Description
INSTANCE-ID	Specifies the MSTP instance identifier. The value is from 0 to 8. The value 0 represents the default instance, CIST.
PRIORITY	Specifies that the bridge priority. The range is from 0 to 61440.

Default

By default, this value is 32768.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

The bridge priority value must be divisible by 4096.

Example

This example shows how to configure the bridge priority value for MSTP instance 2.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#spanning-tree mst 2 priority 0
GA-MLxxTPoE+(config)#
```

12.3 BPDU Guard Commands

12.3.1 spanning-tree bpdu-guard (global)

This command is used to enable the BPDU guard function globally. Use the **no** form of this command to revert to the default setting.

Syntax

- **spanning-tree bpdu-guard**
- **no spanning-tree bpdu-guard**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

In a network, customers do not want all ports of devices to receive STP packets, because some ports that receive STP BPDU packets will cause system resources to be wasted.
If ports are not expected to receive BPDU packets, the BPDU guard function will prevent those ports from receiving BPDU packets. The port where the BPDU guard function is enabled will enter a protection state (drop/block/shutdown) when it receives a STP BPDU packet.
There are 3 mode behaviors when the Switch detects BPDU attacks:

- **Drop -** The Switch drops received STP BPDU packets only, and the port is placed in the normal state.

- **Block -** The Switch drops all received BPDU packets and blocks all data, and the port is placed in the normal state.
- **Shutdown -** The Switch shuts down the port, and the port is placed the error-disabled state.

Example

This example shows how to enable the BPDU guard function globally.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# spanning-tree bpdu-guard
GA-MLxxTPoE+(config)#
```

12.3.2 spanning-tree bpdu-guard (Interface)

This command is used to enable the BPDU guard function on a port. Use the **no** form of this command to disable the BPDU guard function on the port.

Syntax

- **spanning-tree bpdu-guard {drop | block | shutdown}**
- **no spanning-tree bpdu-guard**

Parameters

Parameters	Description
drop	Specifies to drop all received BPDU packets when the interface enters the attacked state.
block	Specifies to drop all packets (include BPDU and normal packets) when the interface enters the attacked state.
shutdown	Specifies to shut down the interface when the interface enters the attacked state.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to enable and configure the BPDU guard operational mode. This command is available for the port and port channel interface configuration.

Example

This example shows how to enable the BPDU Protection function with block mode on GigabitEthernet1/0/1.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# interface gi1/0/1
GA-MLxxTPoE+(config-if)# spanning-tree bpdu-guard block
GA-MLxxTPoE+(config-if)#
```

12.3.3 show spanning-tree bpdu-guard

This command is used to display BPDU guard information.

Syntax

- **show spanning-tree bpdu-guard [interface** *INTERFACE-ID* **[, | -]]**

Parameters

Parameters	Description
interface *INTERFACE-ID*	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display BPDU guard information. If no interface ID is specified, information of all interfaces will be displayed.

Example

This example shows how to display the BPDU guard information and status of interfaces.

```
GA-MLxxTPoE+#show spanning-tree bpdu-guard

 Global State:      Enabled

Interface           State        Mode         Status
--------------      --------     --------     ------------
Gi1/0/1             Enabled      Block        Normal
Gi1/0/2             Disabled     Shutdown     Normal
Gi1/0/3             Disabled     Shutdown     Normal
Gi1/0/4             Disabled     Shutdown     Normal
Gi1/0/5             Disabled     Shutdown     Normal
Gi1/0/6             Disabled     Shutdown     Normal
Gi1/0/7             Disabled     Shutdown     Normal
Gi1/0/8             Disabled     Shutdown     Normal
Gi1/0/9             Disabled     Shutdown     Normal
Gi1/0/10            Disabled     Shutdown     Normal
Gi1/0/11            Disabled     Shutdown     Normal
Gi1/0/12            Disabled     Shutdown     Normal
Gi1/0/13            Disabled     Shutdown     Normal
Gi1/0/14            Disabled     Shutdown     Normal
Gi1/0/15            Disabled     Shutdown     -
Gi1/0/16            Disabled     Shutdown     -
Gi1/0/17            Disabled     Shutdown     -
Gi1/0/18            Disabled     Shutdown     -
Gi1/0/19            Disabled     Shutdown     Normal
--More--
```

This example shows how to display the BPDU guard status of GigabitEthernet1/0/1.

```
GA-MLxxTPoE+#show spanning-tree bpdu-guard interface gi1/0/1

Interface           State        Mode         Status
--------------      --------     --------     ------------
Gi1/0/1             Enabled      Block        Normal

GA-MLxxTPoE+#
```

Display Parameters

Parameters	Description
Interface	Indicates a port channel or a physical port which is not a member of the port channel.
State	Indicates the interface's configuration state.
Mode	Indicates the operation mode of the interface.

Parameters	Description
Status	**Under attack:** BPDU guard is enabled and STP BPDU is detected. **Normal:** BPDU guard is enabled and STP BPDU is not detected.

12.3.4 snmp-server enable traps stp-bpdu-guard

This command is used to enable the sending of SNMP notifications for BPDU guard. Use the **no** form of this command to disable the sending of SNMP notifications for BPDU guard.

Syntax

- **snmp-server enable traps stp-bpdu-guard**
- **no snmp-server enable traps stp-bpdu-guard**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to enable or disable the sending of SNMP notifications for BPDU guard.

Example

This example shows how to enable the sending of SNMP notifications for BPDU guard.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#snmp-server enable traps stp-bpdu-guard
GA-MLxxTPoE+(config)#
```

12.4 RRP (Ring Redundant Protocol) Commands

12.4.1 rrp enable

This command is used to enable the RRP global state. Use the **no** form of this command to revert to the default the function

Syntax

- **rrp enable**
- **no rrp enable**

Parameters

None

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Command Default Level

Level: 12.

Usage Guideline

Use this command enable the RRP global state. Both the RRP global state and RRP domain must be enabled to have RRP working.

Example

This example shows how to enable the RRP global state.

```
GA-MLxxTPoE+# configure terminal
GA-MLxxTPoE+(config)# rrp enable
GA-MLxxTPoE+(config)#
```

12.4.2 timer

This command is used to configure the timer for the RRP domain. Use the **no** form of this command to revert to the default settings.

Syntax

- **timer** {**polling-interval** *SECONDS* | **fail-period** *SECONDS*}
- **no timer** {**polling-interval**| **fail-period**}

Parameters

Parameters	Description
polling-interval *SECONDS*	Specifies the hello time of the RRP domain.
fail-period *SECONDS*	Specifies the fail time of the RRP domain.

Default

The default hello time is 1 second.
The default fail time is 2 seconds.

Command Mode

RRP Configuration Mode

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the timer for the RRP domain. The fail time should be longer than the hello time. If no optional parameter is specified in the no form of this command, both timers will be revert to the default settings.

Example

This example shows how to configure the hello time to 2 seconds and the fail time to 5 seconds.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#rrp domain dom1
GA-MLxxTPoE+(config-rrp)#timer polling-interval 2
GA-MLxxTPoE+(config-rrp)#timer fail-period 5
GA-MLxxTPoE+(config-rrp)#
```

12.4.3 rrp domain

This command is used to create or configure an RRP domain, and enter the RRP configuration mode. Use the **no** form of this command to delete the specified RRP domain.

Syntax

- **rrp domain** *DOMAIN_NAME*
- **no rrp domain** *DOMAIN_NAME*

Parameters

Parameters	Description
DOMAIN_NAME	Specifies the name of the RRP domain with a maximum of 25 characters.

Default

None

Command Mode

Global Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to create, modify or delete an RRP domain, and enter the RRP configuration mode. One domain name represents a physical ring. The Switch supports 8 RRP domains.

Example

This example shows how to create a RRP domain called “dom1”.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#rrp domain dom1
GA-MLxxTPoE+(config-rrp)#
```

12.4.4 control-vlan-id

This command is used to specify the VLAN to be used as control VLAN of the RRP domain. Use the **no** form of this command to remove the configuration.

Syntax

- **control-vlan-id** *VLAN-ID*
- **no control-vlan-id**

Parameters

Parameters	Description
VLAN-ID	Specifies the VLAN ID to be used. The range is from 2 to 4094.

Default

None

Command Mode

RRP Configuration Mode

Command Default Level

Level: 12

Usage Guideline

All nodes of one domain have one control VLAN, and different domains have different control VLANs. The control frame will be sent by using control VLAN. Control VLAN must be newly created, not be displayed or not be operated.

Example

This example shows how to configure control VLAN for the domain called “dom1”

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#rrp domain dom1
GA-MLxxTPoE+(config-rrp)#control-vlan-id 3
GA-MLxxTPoE+(config-rrp)#
```

12.4.5 data-vlan-ids

This command is used to configure VLANs protected by the RRP mechanism. Use the **no** form of this command to delete VLANs

Syntax

- **data-vlan-ids** *VLAN-ID* [, | -]]
- **no data-vlan-ids** *VLAN-ID* [, | -]]

Parameters

Parameters	Description
VLAN-ID	Specifies the VLAN ID to be configured. The range is from 1 to 4094.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen

Default

None

Command Mode

RRP Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to configure or delete VLANs protected by the RRP mechanism.

Example

This example shows how to configure VLANs protected by the RRP mechanism.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#rrp domain dom1
GA-MLxxTPoE+(config-rrp)#data-vlan-ids 100-200
GA-MLxxTPoE+(config-rrp)#
```

12.4.6 type

This command is used to configure the node type.

Syntax

- **type {master |transit}**

Parameters

Parameters	Description
master	Specifies the node as the domain master node. Each RRP domain has one single master node. The master node is responsible for ring polling and ring restoration.
transit	Specifies the node as the domain transit node. Each RRP domain can have multiple transit nodes. The transit node is responsible for link-down alert.

Default

None

Command Mode

RRP Configuration Mode

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the node type.

Example

This example shows how to configure the node type to master for the domain called “dom1”.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#rrp domain dom1
GA-MLxxTPoE+(config-rrp)#type master
GA-MLxxTPoE+(config-rrp)#
```

12.4.7 primary-port

This command is used to configure the first ring port of the RRP domain. Use the **no** form of this command to remove the first ring port.

Syntax

- **primary-port interface** *INTERFACE-ID*
- **no primary-port**

Parameters

Parameters	Description
interface *INTERFACE-ID*	Specifies the interface to be used. The interface can be physical port or port-channel interface.

Default

None

Command Mode

RRP Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Use this command to configure the first ring port of the RRP domain.

Example

This example shows how to configure the GigabitEthernet1/0/4 as the first ring port.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#rrp domain dom1
GA-MLxxTPoE+(config-rrp)#primary-port interface gi1/0/4
GA-MLxxTPoE+(config-rrp)#
```

12.4.8 secondary-port

This command is used to configure the second ring port of the RRP domain. Use the **no** form of this command to remove the second ring port.

Syntax

- **secondary-port interface** *INTERFACE-ID*
- **no secondary-port**

Parameters

Parameters	Description
interface *INTERFACE-ID*	Specifies the interface to be used. The interface can be physical port or port-channel interface.

Default

None

Command Mode

RRP Configuration Mode

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the second ring port of the RRP domain.

Example

This example shows how to configure the GigabitEthernet1/0/2 as the second ring port.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#rrp domain dom1
GA-MLxxTPoE+(config-rrp)#secondary-port interface gi1/0/2
GA-MLxxTPoE+(config-rrp)#
```

12.4.9 ring-guard-port

This command is used to specify the ring guard enabled port. Use the **no** form of this command to disable the function.

Syntax

- **ring-guard-port {primary |secondary |both}**
- **no ring-guard-port**

Parameters

Parameters	Description
primary	Specifies the primary port as the ring guard enabled port.
secondary	Specifies the secondary port as the ring guard enabled port.
both	Specifies both the primary and secondary ports as the ring guard enabled ports.

Default

By default, this option is disabled.

Command Mode

RRP Configuration Mode

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify the ring guard enabled port. When the link of the ring guard enabled port is down, other ports become Blocking.

Example

This example shows how to specify the primary port as the ring guard enabled port.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#rrp domain dom1
GA-MLxxTPoE+(config-rrp)#ring-guard-port primary
GA-MLxxTPoE+(config-rrp)#
```

12.4.10domain

This command is used to enable or disable the RRP domain.

Syntax

- **domain enable**
- **domain disable**

Parameters

None

Default

By default, this option is disabled.

Command Mode

RRP Configuration Mode

Command Default Level

Level: 12

Usage Guideline

Ring ports, control VLAN, data VLAN, and the node type must be configured before the RRP domain is enabled.

Example

This example shows how to enable the RRP domain, dom1.

```
GA-MLxxTPoE+#configure terminal
GA-MLxxTPoE+(config)#rrp domain dom1
GA-MLxxTPoE+(config-rrp)#domain enable
GA-MLxxTPoE+(config-rrp)#
```

12.4.11show rrp

This command is used to display the RRP information.

Syntax

- **show rrp** [*DOMAIN_NAME*]

Parameters

Parameters	Description
DOMAIN_NAME	(Optional) Specifies the name of the RRP domain.

Default

None

Command Mode

User/Privileged EXEC Mode

Command Default Level

Level: 1

Usage Guideline

Use this command to display the RRP information.

Example

This example shows how to display the RRP information.

```
GA-MLxxTPoE+#show rrp

RRP Status : Enabled
Total Domain Number(s) : 1

Domain Name  Ctrl VLAN  Data VLAN(s)                              Ring Status
------------ ---------- ----------------------------------------- -----------
dom1         3          100-200                                   Complete

GA-MLxxTPoE+#
```

13 Appendix - System Log

13.1 Appendix - System Log Entries

13.1.1 802.1X

ID	Log Description	Severity
1.	Event Description: 802.1X Authentication successful. Log Message: [802.1X](<method>) Authorized user <username> (<macaddr>) on Port <portNum> to VLAN <vid> Parameters Description: method: Indicates local or RADIUS. username: The user that is being authenticated. macaddr: The MAC address of the authenticated device. portNum: The switch port number. vid: The authorized VLAN ID.	Informational
2.	Event Description: 802.1X Authentication failure. Log Message: [802.1X](<method>)Rejected user <username> (<macaddr>) on Port <portNum> Parameters Description: method: local or RADIUS. username: TIndicateshe user that is being authenticated. macaddr: The MAC address of the authenticated device. portNum: The switch port number.	Notice
3.	Event Description: The 802.1X authentication table full, cannot authenticate new address. Log Message: [802.1X]Rejected <macaddr> on Port <portNum> (auth table was full) Parameters Description: macaddr: The MAC address of the authenticated device. portNum: The switch port number.	Notice

13.1.2 AAA

ID	Log Description	Severity
1.	Event Description: Successful login. Log Message: Successful login through <Console | Telnet | SSH>(Username: <username>, IP: <ipaddr | ipv6address>) Parameters Description: ipaddr: The IP address. username: The user name. ipv6address: The IPv6 address.	Informational
2.	Event Description: Login failed. Log Message: Login failed through <Console | Telnet | SSH> (Username: <username>, IP: <ipaddr | ipv6address>) Parameters Description: ipaddr: The IP address. username: The user name. ipv6address: The IPv6 address.	Warning
3.	Event Description: Logout. Log Message: Logout through <Console | Telnet | SSH> (Username: <username>, IP: <ipaddr | ipv6address>) Parameters Description: ipaddr: The IP address. username: The user name. ipv6address: The IPv6 address.	Informational
4.	Event Description: Session timed out. Log Message: <Console | Telnet > session timed out (Username: <username>, IP: <ipaddr | ipv6address>) Parameters Description: ipaddr: The IP address. username: The user name. ipv6address: The IPv6 address.	Informational
5.	Event Description: SSH server is enabled. Log Message: SSH server is enabled	Informational
6.	Event Description: SSH server is disabled. Log Message: SSH server is disabled	Informational
7.	Event Description: Authentication Policy is enabled. Log Message: Authentication Policy is enabled (Module: AAA)	Informational
8.	Event Description: Authentication Policy is disabled. Log Message: Authentication Policy is disabled (Module: AAA)	Informational
9.	Event Description: Login failed due to AAA server timeout or improper configuration. Log Message: Login failed through <Console | Telnet | SSH> from <ipaddr | ipv6address> due to AAA server <ipaddr | ipv6address> timeout or improper configuration (Username: <username>) Parameters Description: ipaddr: The IP address. ipv6address: The IPv6 address. username: The user name.	Warning

ID	Log Description	Severity
10.	Event Description: Successful Enable Admin authenticated by AAA local or none or server. Log Message: Successful Enable Admin through <Console | Telnet | SSH> from <ipaddr | ipv6address> authenticated by AAA <local | none | server <ipaddr | ipv6address>> (Username: <username>) Parameters Description: local: Enable admin by AAA local method. none: Enable admin by AAA none method. server: Enable admin by AAA server method. ipaddr: The IP address. ipv6address: The IPv6 address. username: The user name.	Informational
11.	Event Description: Enable Admin failed due to AAA server timeout or improper configuration. Log Message: Enable Admin failed through <Console | Telnet | SSH> from <ipaddr | ipv6address> due to AAA server <ipaddr | ipv6address> timeout or improper configuration (Username: <username>) Parameters Description: ipaddr: The IP address. ipv6address: The IPv6 address. username: The user name.	Warning
12.	Event Description: Enable Admin failed authenticated by AAA local or server. Log Message: Enable Admin failed through <Console | Telnet | SSH> from <ipaddr | ipv6address> authenticated by AAA < local | server <ipaddr | ipv6address>> (Username: <username>) Parameters Description: local: Enable admin by AAA local method. server: Enable admin by AAA server method. ipaddr: The IP address. ipv6address: The IPv6 address. username: The user name.	Warning
13.	Event Description: Successful login authenticated by AAA local or none or server. Log Message: Successful login through <Console | Telnet | SSH> from < ipaddr | ipv6address > authenticated by AAA <local | none | server <ipaddr | ipv6address>> (Username: <username>) Parameters Description: local: Specify AAA local method. none: Specify none method. server: Specify AAA server method. ipaddr: The IP address. ipv6address: The IPv6 address. username: The user name.	Informational
14.	Event Description: Login failed authenticated by AAA local or server. Log Message: Login failed through <Console | Telnet | SSH> from <ipaddr | ipv6address> authenticated by AAA <local | server <ipaddr | ipv6address>> (Username: <username>) Parameters Description: local: Specify AAA local method. server: Specify AAA server method. ipaddr: The IP address. ipv6address: The IPv6 address. username: The user name.	Warning

13.1.3 ARP

ID	Log Description	Severity
1.	Event Description: Gratuitous ARP detected duplicate IP. Log Message: Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>, Interface: <ipif_name>) Parameters Description: ipaddr: The IP address which is duplicated with our device. macaddr: The MAC address of the device that has duplicated IP address as our device. unitID: 1.Interger value; 2.Represent the id of the device in the stacking system. portNum: 1.Interger value; 2.Represent the logic port number of the device. ipif_name: The name of the interface of the switch which has the conflict IP address.	Warning

13.1.4 Authentication (2-step)

ID	Log Description	Severity
1.	Event Description: 2-step Authentication successful. Log Message: [<step-mode>] (<method>) Authorized user <username> (<macaddr>) on Port <portNum> to VLAN <vid> Parameters Description: step-mode: Indicates 2-step authentication mode. method: Indicates local or RADIUS. username: The user that is being authenticated. macaddr: The MAC address of the authenticated device. portNum: The switch port number. vid: The authorized VLAN ID.	Informational
2.	Event Description: MAC-WEB Authentication failures. Log Message: [MAC-WEB] (<method>) Rejected at MAC auth <macaddr>) on Port <portNum> Parameters Description: method: Indicates local or RADIUS. macaddr: The MAC address of the authenticated device. portNum: The switch port number.	Notice
3.	Event Description: MAC-WEB Authentication failures. Log Message: [MAC-WEB] (<method>) Rejected at WEB auth user <username> (<macaddr>) on Port <portNum> Parameters Description: method: Indicates local or RADIUS. username: The user that is being rejected. macaddr: The MAC address of the authenticated device. portNum: The switch port number.	Notice
4.	Event Description: MAC-802.1X Authentication failures. Log Message: [MAC-802.1X] (<method>) Rejected at MAC auth <macaddr>) on Port <portNum> Parameters Description: method: Indicates local or RADIUS. macaddr: The MAC address of the authenticated device. portNum: The switch port number.	Notice
5.	Event Description: MAC-802.1X Authentication failures. Log Message: [MAC-802.1X] (<method>) Rejected at 802.1X auth user <username> (<macaddr>) on Port <portNum> Parameters Description: method: Indicates local or RADIUS. username: The user that is being rejected. macaddr: The MAC address of the authenticated device. portNum: The switch port number.	Notice
6.	Event Description: 802.1 X-WEB Authentication failures. Log Message: [802.1X-WEB] (<method>) Rejected at 802.1X auth user <username> (<macaddr>) on Port <portNum> Parameters Description: method: Indicates local or RADIUS. username: The user that is being rejected. macaddr: The MAC address of the authenticated device. portNum: The switch port number.	Notice

ID	Log Description	Severity
7.	Event Description: 802.1 X-WEB Authentication failures. Log Message: [802.1X-WEB] (<method>) Rejected at WEB auth user <username> (<macaddr>) on Port <portNum> Parameters Description: method: Indicates local or RADIUS. username: The user that is being rejected. macaddr: The MAC address of the authenticated device. portNum: The switch port number.	Notice

13.1.5 BPDU Guard

ID	Log Description	Severity
1.	Event Description: BPDU attack happened. Log Message: Port<portNum> enter BPDU under attacking state (mode: drop / block / shutdown) Parameters Description: portNum: The port number. mode: The BPDU current state.	Informational
2.	Event Description: BPDU attack automatically recover. Log Message: Port <portNum> recover from BPDU under attacking state automatically Parameters Description: portNum: The port number.	Informational
3.	Event Description: BPDU attack manually recover. Log Message: Port<portNum> recover from BPDU under attacking state manually Parameters Description: portNum: The port number.	Informational

13.1.6 DDM

ID	Log Description	Severity
1.	Event description: when the any of SFP parameters exceeds from the warning threshold. Log Message: Optical transceiver <interface-id> <component> <high-low> warning threshold exceeded Parameters description: interface-id: port interface ID. component: DDM threshold type. It can be one of the following types: temperature supply voltage bias current TX power RX power high-low: High or low threshold.	Warning
2.	Event description: when the any of SFP parameters exceeds from the alarm threshold. Log Message: Optical transceiver <interface-id> <component> <high-low> alarm threshold exceeded Parameters description: interface-id: port interface ID. component: DDM threshold type. It can be one of the following types: temperature supply voltage bias current TX power RX power high-low: High or low threshold.	Critical
3.	Event description: when the any of SFP parameters recovers from the warning threshold. Log Message: Optical transceiver <interface-id> <component> back to normal Parameters description: interface-id: port interface ID. component: DDM threshold type. It can be one of the following types: temperature supply voltage bias current TX power RX power	Warning

13.1.7 Debug Error

ID	Log Description	Severity
1.	Event description: system fatal error lead to reboot system. Log Message: System re-start reason: system fatal error	Emergencies
2.	Event description: CPU exception lead to reboot system. Log Message: System re-start reason: CPU exception	Emergencies

13.1.8 DHCPv6 Client

ID	Log Description	Severity
1.	Event description: DHCPv6 client interface administrator state changed. Log Message: DHCPv6 client on interface <ipif-name> changed state to [enabled | disabled] Parameters description: <ipif-name>: Name of the DHCPv6 client interface.	Informational
2.	Event description: DHCPv6 client obtains an ipv6 address from a DHCPv6 server. Log Message: DHCPv6 client obtains an ipv6 address < ipv6address > on interface <ipif-name> Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
3.	Event description: The ipv6 address obtained from a DHCPv6 server starts renewing. Log Message: The IPv6 address < ipv6address > on interface <ipif-name> starts renewing Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
4.	Event description: The ipv6 address obtained from a DHCPv6 server renews success. Log Message: The IPv6 address < ipv6address > on interface <ipif-name> renews success Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
5.	Event description: The ipv6 address obtained from a DHCPv6 server starts rebinding. Log Message: The IPv6 address < ipv6address > on interface <ipif-name> starts rebinding Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
6.	Event description: The ipv6 address obtained from a DHCPv6 server rebinds success. Log Message: The IPv6 address < ipv6address > on interface <ipif-name> rebinds success Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
7.	Event description: The ipv6 address from a DHCPv6 server was deleted. Log Message: The IPv6 address < ipv6address > on interface <ipif-name> was deleted Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational

ID	Log Description	Severity
8.	Event description: DHCPv6 client PD interface administrator state changed. Log Message: DHCPv6 client PD on interface <intf-name> changed state to <enabled | disabled> Parameters description: intf-name: Name of the DHCPv6 client PD interface.	Informational
9.	Event description: DHCPv6 client PD obtains an IPv6 prefix from a delegation router. Log Message: DHCPv6 client PD obtains an ipv6 prefix < ipv6networkaddr> on interface <intf-name> Parameters description: ipv6networkaddr: ipv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
10.	Event description: The IPv6 prefix obtained from a delegation router starts renewing. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts renewing Parameters description: ipv6networkaddr: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
11.	Event description: The IPv6 prefix obtained from a delegation router renews success. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> renews success Parameters description: ipv6anetworkaddr: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
12.	Event description: The IPv6 prefix obtained from a delegation router starts rebinding. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts rebinding Parameters description: ipv6address: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
13.	Event description: The IPv6 prefix obtained from a delegation router rebinds success. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> rebinds success Parameters description: ipv6address: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
14.	Event description: The IPv6 prefix from a delegation router was deleted. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> was deleted Parameters description: ipv6address: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational

13.1.9 DNS Resolver

ID	Log Description	Severity
1.	Event description: Duplicate Domain name cache added, leads a dynamic domain name cache be deleted Log Message: DUPLICATEDDOMAIN: Duplicate Domain name case name: <domain name>, static IP: <static- ip>, dynamic IP:<dynamic-ip > Parameters description: domain name: the domain name string. ipaddr: IP address.	Informational

13.1.10Fan

ID	Log Description	Severity
1.	Event description: Back Fan failed. Log Message: Unit <unitID>, Back Fan <value> failed Parameters description: unitID: The unit ID. value : Fans ID.	Critical
2.	Event description: Back Fan recovered. Log Message: Unit <unitID>, Back Fan <value> back to normal Parameters description: unitID: The unit ID. value : Fans ID.	Critical

13.1.11Interface

ID	Log Description	Severity
1.	Event description: Port link up. Log Message: Port <port> link up, <nway> Parameters description: port: Represents the logical port number. nway: Represents the speed and duplex of link.	Informational
2.	Event description: Port link down. Log Message: Port <port> link down Parameters description: port: Represents the logical port number.	Informational

13.1.12PoE

ID	Log Description	Severity
1.	Event description: Power supply to port has turned on. Log message: Port-<port> Power OFF notification Parameters description: port: Represents the logical port number.	Information
2.	Event description: Power supply to port has turned off. Log message: Port-<port> Power On notification Parameters description: port: Represents the logical port number.	Information
3.	Event description: Feeding power of PoE has exceeded the threshold. Log message: Usage power is above the threshold	Information
4.	Event description: After the feeding power of PoE has exceeded the threshold, it fell below the threshold. Log message: Usage power is below the threshold	Information
5.	Event description: The initialization of PoE IC has failed. Log message: PoE IC Reinit Fail	Information
6.	Event description: PoE IC has reset. Log message: PoE IC Reset	Information

13.1.13PoE Scheduler

ID	Log Description	Severity
1.	Event description: PoE power supply was turned ON by the PoE scheduler. Log message: (PoE) PoE port is changed to ON by PoE Scheduler. Parameters description: port: Represents the logical port number.	Warning
2.	Event description: PoE power supply was turned OFF by the PoE scheduler. Log message: (PoE) PoE port is changed to OFF by PoE Scheduler. Parameters description: port: Represents the logical port number.	Warning
3.	Event description: PoE power supply was turned OFF/ON by the PoE scheduler. Log message: (PoE) PoE port is reset by PoE Scheduler.	Warning

13.1.14PoE Auto Reboot

ID	Log Description	Severity
1.	Event description: Turning OFF/ON of PoE power supply was performed. Log message: Execute PoE OFF/ON Port-<port> Parameters description: port: Represents the logical port number.	Information
2.	Event description: An error of PoE terminal was detected by Ping monitoring. Log message: Detect equipment failure by ICMP <IP> Parameters description: IP: Represents the IP address.	Information
3.	Event description: An error of PoE terminal was detected by LLDP monitoring. Log message: Detect equipment failure by LLDP Port-<port> Parameters description: port: Represents the logical port number.	Information
4.	Event description: An error of PoE terminal was detected by traffic monitoring. Log message: Detect equipment failure by Traffic Port-<port> Parameters description: port: Represents the logical port number.	Information

13.1.15LLDP-MED

ID	Log Description	Severity
1.	Event description: LLDP-MED topology change detected. Log Message: LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>) Parameters description: portNum: The port number. chassisType: chassis ID subtype. Value list: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: chassis ID. portType: port ID subtype. Value list: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: port ID. deviceClass: LLDP-MED device type.	Notice

ID	Log Description	Severity
2.	Event description: Conflict LLDP-MED device type detected. Log Message: Conflict LLDP-MED device type detected (on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>) Parameters description: portNum: The port number. chassisType: chassis ID subtype. Value list: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: chassis ID. portType: port ID subtype. Value list: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: port ID. deviceClass: LLDP-MED device type.	Notice
3.	Event description: Incompatible LLDP-MED TLV set detected. Log Message: Incompatible LLDP-MED TLV set detected (on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>) Parameters description: portNum: The port number. chassisType: chassis ID subtype. Value list: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: chassis ID. portType: port ID subtype. Value list: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: port ID. deviceClass: LLDP-MED device type.	Notice

13.1.16Loop Detection

ID	Log Description	Severity
1.	Event description: The loop detected between 2 ports or 2 LACP interfaces. Log Message: The loop detected between port/port-channel <portNum> and <portNum> Parameters description: portNum: The port number or LACP interface id.	Warning
2.	Event description: The loop detected on 1 port or 1 LACP interface. Log Message: The loop detected on port/port-channel <portNum> Parameters description: portNum: The port number or LACP interface id.	Warning
3.	Event description: The loop detected between 1 port and 1 LACP interface. Log Message: The loop detected between port/port-channel <portNum> and port/port-channel <portNum> Parameters description: portNum: The port number or port-channel number.	Warning
4.	Event description: Looped port or LACP interface auto recovery. Log Message: Port/Port-channel <portNum> auto recovery Parameters description: portNum: The port number or LACP interface id.	Informational

13.1.17MAC-based Access Control

ID	Log Description	Severity
1.	Event description: MAC authentication successful. Log Message: [MAC](<method>)Authorized <macaddr> on Port <portNum> to VLAN <vid> Parameters description: method: Indicates local or RADIUS. macaddr: The MAC address of the authenticated device. portNum: The switch port number. vid: The authorized VLAN ID.	Informational
2.	Event description: MAC authentication failure. Log Message: [MAC](<method>)Rejected <macaddr> on Port <portNum> Parameters description: method: Indicates local or RADIUS. macaddr: The MAC address of the authenticated device. portNum: The switch port number.	Notice
3.	Event description: The MAC authentication table full, cannot authenticate new address. Log Message: [MAC]Rejected <macaddr> on Port <portNum> (auth table was full) Parameters description: macaddr: The MAC address of the authenticated device. portNum: The switch port number.	Notice

13.1.18MSTP Debug Enhancement

ID	Log Description	Severity
1.	Event description: Topology changed. Log Message: Topology changed (Instance : <Instance-id>,<interface-id>, MAC:<macaddr>) Parameters description: Instance-id: Instance ID. interface-id: Port ID. macaddr: MAC address.	Notice
2.	Event description: Spanning Tree new Root Bridge. Log Message: [CIST | CIST Regional | MSTI Regional] New Root bridge selected ([Instance: <Instance-id>] MAC: <macaddr> Priority :< priority>) Parameters description: Instance-id : Instance ID. macaddr: MAC address. priority: Priority value.	Notice
3.	Event description: Spanning Tree Protocol is enabled. Log Message: Spanning Tree Protocol is enabled	Informational
4.	Event description: Spanning Tree Protocol is disabled. Log Message: Spanning Tree Protocol is disabled	Informational
5.	Event description: New root port. Log Message: New root port selected (Instance:<instance-id>, <interface-id >) Parameters description: instance-id: Instance ID. interface-id: Port ID.	Notice
6.	Event description: Spanning Tree port status changed. Log Message: Spanning Tree port status change (Instance :< instance-id>, <interface-id>) <old-status> -> <new-status> Parameters description: instance-id: Instance ID. interface-id: Port ID. old_status: Old status. new_status: New status.	Notice
7.	Event description: Spanning Tree port role changed. Log Message: Spanning Tree port role change (Instance :< instance-id>, <interface-id>) <old-role> -> <new-role> Parameters description: instance-id: Instance ID. interface-id: Port ID. old_role: Old role. new_status: New role.	Informational
8.	Event description: Spanning Tree instance created. Log Message: Spanning Tree instance created. (Instance :< instance-id>) Parameters description: instance-id: Instance ID.	Informational
9.	Event description: Spanning Tree instance deleted. Log Message: Spanning Tree instance deleted. (Instance :< instance-id >) Parameters description: instance-id: Instance ID.	Informational

ID	Log Description	Severity
10.	Event description: Spanning Tree Version changed. Log Message: Spanning Tree version change (new version :< new-version>) Parameters description: new_version: New STP version.	Informational
11.	Event description: Spanning Tree MST configuration ID name and revision level changed. Log Message: Spanning Tree MST configuration ID name and revision level change (name :< name>, revision level <revision-level>) Parameters description: name : New name. revision_level: New revision level.	Informational
12.	Event description: Spanning Tree MST configuration ID VLAN mapping table deleted. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: < instance-id > delete vlan <startvlanid> [- <endvlanid>]) Parameters description: instance-id: Instance ID. startvlanid-endvlanid: VLAN list.	Informational
13.	Event description: Spanning Tree MST configuration ID VLAN mapping table added. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: < instance-id > add vlan <startvlanid> [- <endvlanid>]) Parameters description: instance-id: Instance ID. startvlanid-endvlanid: VLAN list.	Informational
14.	Event description: Spanning Tree role changed due to the guard root function. Log Message: Spanning Tree port role change (Instance : < instance-id >, <interface-id>) to alternate port due to the guard root Parameters description: instance-id: Instance ID. interface-id: Port ID.	Informational

13.1.19Port Security

ID	Log Description	Severity
1.	Event description: Address full on a port Log Message: MAC address <mac-address> causes port security violation on <interface-id> Parameters description: macaddr: The violation MAC address. interface-id: The interface on which the violation occur.	Warning
2.	Event description: Address full on system. Log Message : Limit on system entry number has been exceeded	Warning

13.1.20RADIUS

ID	Log Description	Severity
1.	Event description: This log will be generated when RADIUS assigned a valid VLAN ID attributes. Log Message: RADIUS server <server-ip> assigned VID: <vid> to port <interface-id> (Username: <username>) Parameters description: server-ip: It indicates the RADIUS server IP address. vid: The assign VLAN ID that authorized by from RADIUS server. interface-id: It indicates the port number of the client authenticated. username: It indicates the username for authentication.	Informational
2.	Event description: This log will be generated when RADIUS assigned a valid bandwidth attributes. Log Message: RADIUS server <server-ip> assigned <direction> bandwidth: <threshold> to port < interface-id> (Username: <username>) Parameters description: server-ip: It indicates the RADIUS server IP address. direction: It indicates the direction for bandwidth control, e.g.: ingress or egress. threshold: The assign threshold of bandwidth that authorized by from RADIUS server. interface-id: It indicates the port number of the client authenticated. username: It indicates the username for authentication.	Informational
3.	Event description: This log will be generated when RADIUS assigned a valid priority attributes. Log Message: RADIUS server <server-ip> assigned 802.1p default priority: <priority> to port < interface-id> (Username: <username>) Parameters description: server-ip: It indicates the RADIUS server IP address. priority: The assign priority that authorized by from RADIUS server. interface-id: It indicates the port number of the client authenticated. username: It indicates the username for authentication.	Informational
4.	Event description: This log will be generated when RADIUS assigned ACL script but fails to apply to the system due to insufficient resource. Log Message: RADIUS server <server-ip> assigns <username> ACL failure at port < interface-id> (<acl-script>) Parameters description: server-ip: It indicates the RADIUS server IP address. username: It indicates the username for authentication. interface-id: It indicates the port number of the client authenticated. acl-script: The assign ACL script that authorized by from RADIUS server.	Warning
5.	Event description: This log will be generated when fail to assign access-list number. Log Message: Local assigns [USERNAME] filter-id ID failure at port INTERFACE-ID Parameters description: username: It indicates the username for authentication. filter-id: It indicates access-list number. interface-id: It indicates the port number of the client authenticated.	Warning

13.1.21RRP

ID	Log Description	Severity
1.	Event description: The status in “Master Node” changes from “Failed” to “Complete. Log Message: Ring topology was recovered to complete	Notice
2.	Event description: The status in “Master Node” changes from “Complete” to “Failed. Log Message: Ring topology was failed	Warning
3.	Event description: Master or Transit node flush its Forwarding Database based on RRP packets or state machine. Log Message: FDB was flushed	Informational
4.	Event description: The RRP status in “Transit Node” changes to “Link-Up. Log Message: RRP ring status was changed to Link-Up	Warning
5.	Event description: The RRP status in “Transit Node” changes to “Link-Down. Log Message: RRP ring status was changed to Link-Down	Notice
6.	Event description: The RRP status in “Transit Node” changes to “Pre-Forwarding”. Log Message: RRP ring status was changed to Pre-Forwarding	Informational
7.	Event description: Worked ring guard function at the specific domain and port. Log Message: Ring Guard was activated on “<domain-name>” domain at port <port> Parameters description: <domain name>: target domain name. <port num>: target port number worked ring guard function.	Informational

13.1.22SNMP

ID	Log Description	Severity
1.	Event Description: SNMP request received with invalid community string. Log Message: SNMP request received from <ipaddr> with invalid community string Parameters Description: ipaddr: The IP address.	Informational

13.1.23System

ID	Log Description	Severity
1.	Event description: System start up. Log Message: [Unit <unitID>,] System started up Parameters description: unitID: The unit ID.	Critical
2.	Event description: Save current configuration to flash. Log Message: [Unit <unitID>,] Configuration saved to flash by console (Username: <username>) Parameters description: unitID: The unit ID. username: The user name.	Informational
3.	Event description: Power fail. Log Message: Unit <unitID> Power <powerID> failed Parameters description: unitID: The unit ID. powerID: The power ID.	Critical
4.	Event description: Power is recovered. Log Message: Unit <unitID> Power <powerID> back to normal Parameters description: unitID: The unit ID. powerID: The power ID.	Critical
5.	Event description: Save system configuration from remote. Log Message: [Unit <unitID>,] Configuration saved to flash (Username: <username>, IP: <ipaddr>) Parameters description: unitID: The unit ID. username: The user name. ipaddr: The ip address.	Informational
6.	Event description: System power up and start up. Log Message: [Unit <unitID>,] System cold start Parameters description: unitID: The unit ID.	Critical
7.	Event description: System reboot and start up. Log Message: [Unit <unitID>,] System warm start Parameters description: unitID: The unit ID.	Critical

13.1.24SNTP

ID	Log Description	Severity
1.	Event description: Shows the time when the clock synchronization of SNTP was performed. Log message: SNTP first update to YYYY/MM/DD hh:mm:ss	Information

13.1.25Telnet

ID	Log Description	Severity
1.	Event description: Successful login through Telnet. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Informational
2.	Event description: Login failed through Telnet. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Warning
3.	Event description: Logout through Telnet. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Informational
4.	Event description: Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>) Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Informational

13.1.26Temperature

ID	Log Description	Severity
1.	Event description: Temperature sensor enters alarm state. Log Message: Uint <unitID> Sensor:<sensorID> detects abnormal temperature <temperature> Parameters description: unitID: The unit ID. sensorID: The sensor ID. temperature: The current temperature of the sensor.	Critical
2.	Event description: Temperature recovers to normal. Log Message: Uint <unitID> Sensor:<sensorID> temperature back to normal Parameters description: unitID: The unit ID. sensorID: The sensor ID. temperature: The temperature.	Critical

13.1.27Traffic Control

ID	Log Description	Severity
1.	Event description: Broadcast, Multicast or Unicast storm occurrence. Log Message: Broadcast | Multicast | Unicast> storm is occurring on <interface-id> Parameters description: interface-id: The interface ID on which a storm is occurring.	Warning
2.	Event description: Broadcast, Multicast or Unicast storm cleared. Log Message: <Broadcast | Multicast | Unicast> storm is cleared on <interface-id> Parameters description: interface-id: The interface ID on which a storm is cleared.	Informational
3.	Event description: Port shut down due to a packet storm. Log Message: <interface-id> is currently shut down due to the <Broadcast | Multicast | Unicast> storm Parameters description: Interface-id: The interface ID on which is error-disabled by storm.	Warning

13.1.28Voice VLAN

ID	Log Description	Severity
1.	Event description: When a new voice device is detected on an interface. Log Message: New voice device detected (<interface-id>, MAC: < mac-address >) Parameters description: interface-id: Interface name. mac-address: Voice device MAC address	Informational
2.	Event description: When an interface which is in auto voice VLAN mode joins the voice VLAN. Log Message: < interface-id > add into voice VLAN <vid > Parameters description: interface-id: Interface name.s vid: VLAN ID.	Informational
3.	Event description: When an interface leaves the Voice VLAN and at the same time, no voice device is detected in the aging interval for that interface, the log message will be sent. Log Message: < interface-id > remove from voice VLAN <vid > Parameters description: interface-id: Interface name. vid: LAN ID.	Informational

14 Appendix - System Trap

14.1 Appendix - System Trap Entries

14.1.1 BPDU Guard

ID	Trap Name	Trap Description	OID
1.	mnoBpduProtectionUnderAttackingTrap	BPDU attack happened, enter drop / block / shutdown mode. Binding objects: mnoBpduProtectionPortIndex The port interface. (2) mnoBpduProtectionPortMode Drop / block / shutdown mode.	1.3.6.1.4.1.396.5.5.3.4.0.1
2.	mnoBpduProtectionRecoveryTrap	BPDU attack automatically recover. Binding objects: mnoBpduProtectionPortIndex The port interface. mnoBpduProtectionRecoveryMethod Auto/manual recovers.	1.3.6.1.4.1.396.5.5.3.4.0.2

14.1.2 DDM

ID	Trap Name	Trap Description	OID
1.	mnoDdmAlarmTrap	The trap is sent when any parameter value exceeds the alarm threshold value or recovers to normal status depending on the configuration of the trap action. Binding objects: mnoDdmPort The port number mnoDdmThresholdType The ddm threshold type temperature/voltage/bias/txpower/rxpower mnoDdmThresholdExceedType The threshold that was exceeded was a high alarm threshold or a low alarm threshold (4) mnoDdmThresholdExceedOrRecover The FiberModule is exceeding its ddm threshold or recover to normal status	1.3.6.1.4.1.396.5.5.1.4.0.1
2.	mnoDdmWarningTrap	The trap is sent when any parameter value exceeds the warning threshold value or recovers to normal status depending on the configuration of the trap action. Binding objects: mnoDdmPort The port number mnoDdmThresholdType The ddm threshold type temperature/voltage/bias/txpower/rxpower mnoDdmThresholdExceedType The threshold that was exceeded was a high warning threshold or a low warning threshold (4) mnoDdmThresholdExceedOrRecover The FiberModule is exceeding its ddm threshold or recover to normal status	1.3.6.1.4.1.396.5.5.1.4.0.2

14.1.3 DHCP Server Protect

ID	Trap Name	Trap Description	OID
1.	mnoFilterDetectedTrap	Send trap when an illegal DHCP server is detected. The same illegal DHCP server IP address detected is just sent once to the trap receivers within the log ceasing unauthorized duration. Binding objects: mnoFilterDetectedIP The illegal DHCP server IP address. mnoFilterDetectedport The port interface.	1.3.6.1.4.1.396.5.5.3.7.0.1

14.1.4 Fan

ID	Trap Name	Trap Description	OID
1.	mnoFanFailure	This notification will send out when the fan failure.	1.3.6.1.4.1.396.5.5.1.1
2.	mnoFanRecovery	This notification will send out when the fan recovery.	1.3.6.1.4.1.396.5.5.1.5

14.1.5 Gratuitous ARP

ID	Trap Name	Trap Description	OID
1.	mnoAgentGratuitousARPTrap	The trap is sent when IP address conflicted. Binding objects: agentGratuitousARPIpAddr The conflicted IP address received in the gratuitous ARP packet. agentGratuitousARPMacAddr The sender's MAC address in the gratuitous ARP packet. agentGratuitousARPPortNumber The switch's port number who received the gratuitous ARP packet. agentGratuitousARPInterfaceName The switch's IP interface name who received the gratuitous ARP.	1.3.6.1.4.1.396.5.5.3.6.0.1

14.1.6 LLDP-MED

ID	Trap Name	Trap Description	OID
1.	lldpRemTablesChange	A lldpRemTablesChange notification is sent when the value of lldpStatsRemTableLastChangeTime changes. Binding objects: (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts	1.0.8802.1.1.2.0.0.1
2.	lldpXMedTopologyChangeDetected	A notification generated by the local device sensing a change in the topology that indicates that a new remote device attached to a local port, or a remote device disconnected or moved from one port to another. Binding objects: (1) lldpRemChassisIdSubtype (2) lldpRemChassisId (3) lldpXMedRemDeviceClass	1.0.8808.1.1.2.1.5.4795.0.1

14.1.7 Loop Detect

ID	Trap Name	Trap Description	OID
1.	mnoLoopDetectNotification	Indicates the network loop occurred.	1.3.6.1.4.1.396.5.5.2.1
2.	mnoLoopRecoveryNotification	Indicates the network loop resolved.	1.3.6.1.4.1.396.5.5.2.2

14.1.8 MAC-based Access Control

ID	Trap Name	Trap Description	OID
1.	mnoMacBasedAccessControlLoggedSuccess	The trap is sent when a MAC-based Access Control host is successfully logged in. Binding objects: mnoMacBasedAuthInfoMacIndex The host MAC addresses. mnoMacBasedAuthInfoPortIndex The port interface. mnoMacBasedAuthVID The VLAN ID.	1.3.6.1.4.1.396.5.5.3.2.0.1
2.	mnoMacBasedAccessControlLoggedFail	The trap is sent when a MAC-based Access Control host login fails. Binding objects: mnoMacBasedAuthInfoMacIndex The host MAC addresses. mnoMacBasedAuthInfoPortIndex The port interface. mnoMacBasedAuthVID The VLAN ID.	1.3.6.1.4.1.396.5.5.3.2.0.2
3.	mnoMacBasedAccessControlAgesOut	The trap is sent when a MAC-based Access Control host ages out. Binding objects: mnoMacBasedAuthInfoMacIndex The host MAC addresses. (2) mnoMacBasedAuthInfoMacIndex The port interface. (3) mnoMacBasedAuthVID The VLAN ID.	1.3.6.1.4.1.396.5.5.3.2.0.3

14.1.9 MAC Notification

ID	Trap Name	Trap Description	OID
1.	mnoL2macNotification	This trap indicates the MAC addresses variation in address table Binding objects: mnoL2macNotifyInfo Devices MAC address change information. And the detailed information include : Operation Code + MAC address + Box ID + Interface ID + Zero. Operation Code: 1, 2 1 means learned a new MAC address 2 means deleted an old MAC address. Box ID: The switch box ID Interface ID: The Interface ID learned or deleted on the box. Zero: Used to separate each message (Operate Code + MAC address + Box ID + Port Number).	1.3.6.1.4.1.396 .5.5.3.1.0.1

14.1.10MSTP

ID	Trap Name	Trap Description	OID
1.	newRoot	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional.	1,3,6,1,2,1,17.0.1
2.	topologyChange	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation ofthis trap is optional	1,3,6,1,2,1,17.0.2

14.1.11 Port Security

ID	Trap Name	Trap Description	OID
1.	mnoL2PortSecurityViolationTrap	When the port security trap is enabled, new MAC addresses that violate the pre-defined port security configuration will trigger trap messages to be sent out. Binding objects: mnoPortSecPortIndex The port interface. mnoL2PortSecurityViolationMac The host MAC addresses.	1.3.6.1.4.1.396.5.5.3.3.0.1

14.1.12Port

ID	Trap Name	Trap Description	OID
1.	linkUp	A notification is generated when port linkup. Binding objects: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6. 3.1.1.5.4
2.	linkDown	A notification is generated when port linkdown. Binding objects: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6. 3.1.1.5.3

14.1.13PoE

ID	Trap Name	Trap Description	OID
1.	pethPsePortOnOffNotification	Shows that the power supply to PoE port has started/stopped.	1.3.6.1.2.1.105.0.1
2.	pethMainPowerUsageOnNotification	Shows that the power supply capacity exceeded the set power supply threshold.	1.3.6.1.2.1.105.0.2
3.	pethMainPowerUsageOffNotification	Shows that the power supply capacity fell below the set power supply threshold.	1.3.6.1.2.1.105.0.3

14.1.14PoE Auto Reboot

ID	Trap Name	Trap Description	OID
1.	EventFailureNotification	Shows that the PoE auto reboot judged the terminal as abnormal.	1.3.6.1.4.1.396.5.5.1.9.1
2.	EventRecoverNotification	Shows that the PoE auto reboot judged the terminal as normal.	1.3.6.1.4.1.396.5.5.1.9.2

14.1.15RMON

ID	Trap Name	Trap Description	OID
1.	risingAlarm	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps. Binding objects: (1)alarmIndex (2)alarmVariable (3)alarmSampleType (4) alarmValue (5) alarmRisingThreshold	1.3.6.1.2.1.16 .0.1
2.	fallingAlarm	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps. Binding objects: (1)alarmIndex (2) alarmVariable (3)alarmSampleType (4)alarmValue (5) alarmFallingThreshold	1.3.6.1.2.1.16 .0.2

14.1.16SNMP Authentication

ID	Trap Name	Trap Description	OID
1.	authenticationFailure	An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.	1.3.6.1.6. 3.1.1.5.5

14.1.17System

ID	Trap Name	Trap Description	OID
1.	coldStart	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.	1.3.6.1.6.3.1.1.5.1
2.	warmStart	A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.	1.3.6.1.6.3.1.1.5.2

14.1.18Temperature

ID	Trap Name	Trap Description	OID
1.	mnoTemperatureRising Alarm	This notification will send out when current temperature more than high threshold.	1.3.6.1.4.1.396.5.5.1.2.1
2.	mnoTemperatureFalling Alarm	This notification will send out when current temperature falling from high threshold.	1.3.6.1.4.1.396.5.5.1.2.2

14.1.19Traffic Control

ID	Trap Name	Trap Description	OID
1.	mnoPktStormOccurred	When packet storm is detected by packet storm mechanism and take shutdown as action. Binding objects: mnoPktStormCtrlPortIndex The port interface.	1.3.6.1.4.1.396.5.5.3.5.0.1
2.	mnoPktStormCleared	When the packet storm is clear. Binding objects: mnoPktStormCtrlPortIndex The port interface.	1.3.6.1.4.1.396.5.5.3.5.0.2
3.	mnoPktStormDisablePort	When the port is disabled by the packet storm mechanism. Binding objects: mnoPktStormCtrlPortIndex The port interface.	1.3.6.1.4.1.396.5.5.3.5.0.3

Panasonic Electric Works Networks Co., Ltd.

2-12-7, Higashi-Shimbashi, Minato-ku, Tokyo Japan, 105-0021
URL: https://panasonic.co.jp/ew/pewnw/english/index.html

P1019-12025