

# **GEPON OLT CLI USER MANUAL**

**Version V1.9**

**Release Date 2021-4-25**

## Contents

1.	Access to OLT .....	10
1.1	Access to OLT CLI via console cable .....	10
1.2	Configuring the Switch for Secure Shell .....	11
1.2.1	Understanding SSH .....	11
1.2.2	Configuring SSH .....	12
1.2.3	Displaying the SSH Configuration and Status .....	14
2.	Command Line Interface .....	15
2.1	Abstract .....	15
2.2	CLI configuration mode .....	15
2.3	CLI specialities .....	15
1.2.4	Online help .....	15
1.2.5	Display specialities .....	18
1.2.6	History commands .....	18
1.2.7	Error messages .....	18
1.2.8	Edit specialities .....	18
3.	Port Configuration .....	20
3.1	Port configuration .....	20
3.1.1	Enter port configure mode .....	20
3.1.2	Enable /Disable port .....	20
3.1.3	Configure port description .....	21
3.1.4	Configure port duplex mode .....	21
3.1.5	Configure port speed .....	22
3.1.6	Configure port rate limitation .....	22
3.1.7	Configure port VLAN mode .....	22
3.1.8	Configure hybrid port VLAN .....	23
3.1.9	Configure trunk port VLAN .....	24
3.1.10	Configure port PVID .....	24
3.1.11	Configure access port VLAN .....	24
3.1.12	Configure port flow control .....	25
3.1.13	Configure port broadcast suppression .....	25
3.1.14	Configure port multicast suppression .....	26
3.1.15	Configure port unknown unicast suppression .....	26
3.1.16	Configure port isolation .....	27
3.1.17	Configure port loopback .....	27
3.1.18	Configure port loopback detection .....	28
3.1.19	Configure port jumboframe .....	28
3.1.20	Show port statistics .....	28
3.1.21	Clean port statistics .....	29
3.1.22	Show interface configurations .....	29
3.1.23	Set to 10G mode .....	30
3.2	Example .....	30
4.	Port Aggregation Configuration .....	32

4.1	Introduction	32
4.2	Port Aggregation Configuration	32
4.2.1	Create static aggregation group	32
4.2.2	Configure load balancing policy of aggregation group	32
4.2.3	Configure member port of aggregation group	33
5.	VLAN Configuration	34
5.1	VLAN configuration	34
5.1.1	Create/Delete VLAN	34
5.1.2	Configure/delete VLAN description	34
5.1.3	Configure/delete IP address and mask of VLAN	35
5.2	Show VLAN information	35
6.	VLAN Translation/QinQ	37
6.1	Configure VLAN translation/QinQ	37
6.2	Example	37
7.	MAC Address Configuration	39
7.1	Overview	39
7.2	Configure MAC address	39
7.2.1	Configure MAC address table	39
7.2.2	Configure MAC address aging time	40
7.2.3	Clean MAC address table	40
7.2.4	Configure maximum learnt MAC entries of port	40
7.3	Show MAC address table	41
7.3.1	Show MAC address table	41
7.3.2	Show MAC address aging time	41
7.4	Configure MAC flapping	41
7.4.1	Configure MAC flapping status	41
7.4.2	Configure MAC flapping interval	42
7.4.3	Configure MAC flapping Mode	42
7.4.4	Configure MAC flapping Range	42
7.4.5	Configure MAC flapping suppression	43
7.4.6	Configuring MAC flapping port status	43
7.4.7	Clear MAC flapping Table	43
7.5	Show MAC flapping	44
7.5.1	Show MAC flapping information	44
7.5.2	Show MAC flapping port status	44
8.	Configure Port Mirroring	45
8.1	Configure mirroring destination port	45
8.2	Configure mirroring source port	45
8.3	Delete port mirroring	46
9.	IGMP Configuration	47
9.1	IGMP Snooping	47
9.1.1	Enable/disable IGMP Snooping	47
9.1.2	Configure multicast data forwarding mode	47
9.1.3	Configure port multicast VLAN	47

9.1.4	Configure multicast router port .....	48
9.1.5	Configure static multicast .....	48
9.1.6	Configure fast leave .....	48
9.1.7	Configure multicast group limit .....	49
9.1.8	Configure parameters of special query .....	49
9.1.9	Configure parameters of general query .....	50
9.1.10	Configure source IP of query .....	50
9.1.11	Configure multicast member aging time .....	50
9.1.12	Show multicast group information .....	51
9.2	Example .....	51
10.	ACL Configuration .....	53
10.1	Overview .....	53
10.2	ACL configuration .....	53
10.2.1	IP standard ACL .....	53
10.2.2	IP extended ACL .....	54
10.2.3	ACL based on MAC address .....	54
10.2.4	ACL based on port binding .....	55
10.2.5	ACL based on QoS .....	56
10.2.6	ACL rule apply to port .....	56
10.3	Example .....	57
11.	QoS Configuration .....	58
11.1	Configure queue scheduling mode .....	58
11.2	Configure queue mapping .....	58
12.	STP Configuration .....	60
12.1	STP default settings .....	60
12.2	Configure STP .....	60
12.2.1	Enable device's STP function .....	60
12.2.2	Enable port STP .....	61
12.2.3	Configure spanning tree mode .....	61
12.2.4	Configure bridge priority .....	61
12.2.5	Configure forward delay .....	62
12.2.6	Configure hello time .....	62
12.2.7	Configure max age time .....	63
12.2.8	Configure priority of designated port .....	63
12.2.9	Configure path cost of designated port .....	64
12.2.10	Configure edge port .....	64
12.2.11	Configure point to point mode .....	65
12.3	Show STP information .....	65
13.	OLT Management Configuration .....	67
13.1	Configure outband management .....	67
13.1.1	Enter AUX port configuration mode .....	67
13.1.2	Configure outband management IP address and mask .....	67
13.1.3	Configure Outband Management IPv6 Address .....	67
13.1.4	Show AUX port information .....	68

13.2	Configure inband management .....	68
13.3	Configure management gateway .....	69
14.	L3 Route Configuration .....	70
14.1	Configuring L3 Interface .....	70
14.2	ARP Proxy.....	70
14.3	Static Route.....	71
14.4	RIP Configuration .....	71
14.4.1	Configuring Basic RIP Parameters.....	71
14.4.2	Configuring RIP Authentication.....	73
14.4.3	Configuring Split Horizon.....	74
14.4.4	Configuring RIP v1/2 Compatible .....	75
14.5	OSPF Configuration .....	76
14.5.1	Configuring Basic OSPF Parameters .....	76
14.5.2	Configuring OSPF Interfaces .....	76
14.5.3	Configuring OSPF Area Parameters .....	78
14.5.4	Configuring OSPF Other Parameters.....	80
14.5.5	Monitoring OSPF .....	81
14.6	Manipulate routing selection updates .....	82
14.6.1	Routing IP List.....	82
14.6.2	Route Redistribution.....	84
14.6.3	Use The Distribution List To Control Routing Selection Updates .....	87
14.6.4	Use Routing Mapping Tables To Control Routing Selection Updates...	92
14.6.5	Filter Routing Using Prefix Lists .....	95
15.	DHCP Management Configuration .....	97
15.1	Configure DHCP server.....	97
15.2	Configure DHCP relay.....	97
15.3	Configure DHCP Snooping .....	99
15.4	Configuring IP Source Guard.....	101
15.4.1	Understanding IP Source Guard.....	101
15.4.2	Configuring IP Source Guard .....	102
15.4.3	Configuring IP Source Guard for Static Hosts on a Layer 2 Access Port	104
16.	IPv6.....	106
16.1	VLAN IPv6 Address.....	106
16.1.1	Configure/delete VLAN IPv6 address.....	106
16.2	IPv6 Static Neighbour.....	106
16.3	IPv6 SLAAC .....	107
16.3.1	IPv6 SLAAC Work processes .....	107
16.3.2	IPv6 SLAAC Configuration.....	108
16.3.3	Example(pending).....	110
16.4	DHCPv6 .....	110
16.4.1	DHCPv6 overview.....	110
16.4.2	DHCPv6 Server .....	112
16.4.3	DHCPv6 Relay .....	117
16.5	IPv6 Route .....	119

16.5.1 IPv6 static route configuration.....	119
16.5.2 View IPv6 hardware routing information.....	120
16.6 IPv6 Connectivity Test.....	120
17. PON Management Configuration .....	122
17.1 Enable/Disable PON.....	122
17.2 PON downstream encryption.....	122
17.3 Configure maximum RTT.....	123
17.4 PON ONU laser detect .....	123
17.5 Show PON port statistics.....	123
17.6 Show optical module parameters and alarms .....	124
18. ONU Management Configuration .....	125
18.1 ONU basic configuration.....	125
18.1.1 Configure ONU authentication mode.....	125
18.1.2 Remove authorized ONU .....	125
18.1.3 Deregister or reset ONU.....	126
18.1.4 Configure ONU authorization MAC list .....	126
18.1.5 Configure ONU authorization LOID list.....	126
18.1.6 Measure ONU distance.....	127
18.1.7 Configure ONU description string.....	127
18.1.8 Configure ONU downstream encryption .....	127
18.1.9 Configure ONU upstream bandwidth.....	127
18.1.10 Configure ONU downstream bandwidth.....	128
18.1.11 Configure ONU MAC limit .....	128
18.1.12 Show ONU status .....	129
18.1.13 Show ONU statistics .....	129
18.2 ONU global configuration .....	129
18.2.1 Show ONU information .....	129
18.2.2 Update ONU image.....	130
18.2.3 Auto upgrade ONU.....	130
18.2.4 Configure ONU management IP.....	131
18.2.5 Configure ONU SNMP .....	131
18.2.6 Configure ONU multi LLID.....	132
18.2.7 Configure ONU primary PON interface.....	132
18.2.8 Configure ONU FEC function .....	132
18.2.9 Configure optical link protection .....	133
18.2.10 Configure ONU SLA function .....	133
18.2.11 Configure ONU multicast mode .....	133
18.2.12 Configure ONU fast leave function.....	134
18.2.13 Restart ONU .....	134
18.2.14 Configure ONU power saving mode .....	134
18.2.15 Configure ONU sleep duration and wake up duration .....	135
18.2.16 Configure ONU optical link protection mechanism .....	135
18.2.17 Configure ONU PON power supply control .....	136
18.2.18 Configure ONU MAC aging time .....	136

18.2.19	Configure ONU PON port performance statistics .....	137
18.2.20	Clear/show ONU PON port statistics.....	137
18.3	ONU port configuration.....	137
18.3.1	Show onu port information .....	137
18.3.2	Enable/Disable ONU port.....	138
18.3.3	Configure ONU port autonegotiation .....	138
18.3.4	Configure ONU port re-autonegotiation.....	138
18.3.5	Configure ONU port upstream policy.....	139
18.3.6	Configure ONU port downstream rate limit.....	139
18.3.7	Configure ONU port flow control.....	139
18.3.8	Configure ONU port loopback detection .....	140
18.3.9	Configure ONU loop port auto-shutdown.....	140
18.3.10	Configure ONU port VLAN mode.....	140
18.3.11	Configure ONU port PVID.....	141
18.3.12	Configure ONU port VLAN translation entries .....	141
18.3.13	Configure ONU port VLAN trunk entries .....	141
18.3.14	Configure ONU port VLAN aggregation entries.....	142
18.3.15	Show ONU port VLAN configurations .....	142
18.3.16	Configure ONU port QoS function.....	142
18.3.17	Configure ONU port multicast VLAN.....	143
18.3.18	Configure ONU port maximum multicast groups .....	143
18.3.19	Configure ONU port multicast VLAN strip .....	144
18.3.20	Configure ONU port statistics .....	144
18.3.21	Clear/Show ONU port statistics.....	145
18.4	ONU remote voice configuration.....	145
18.4.1	Show basic information .....	145
18.4.2	Configure global parameters .....	145
18.4.3	Enable/disable POTS port.....	146
18.4.4	Configure H.248 protocol .....	146
18.4.5	Configure POTS UserTID information(H.248) .....	147
18.4.6	Configure RTP TID information(H.248).....	147
18.4.7	Configure SIP protocol .....	147
18.4.8	Configure SIP account parameters of POTS.....	148
18.4.9	Configure fax mode.....	148
18.4.10	VoIP module operation.....	149
18.4.11	Configure SIP digitmap.....	149
18.5	ONU remote alarm information.....	149
18.5.1	Show onu alarm information.....	149
18.5.2	Show onu pon alarm information.....	150
18.5.3	Show onu port alarm information.....	151
18.5.4	Show onupots alarm information .....	152
18.5.5	Show onu E1 alarm information .....	152
18.6	ONU remote private oam configuration.....	152
18.6.1	Show ONU version of software hardware.....	152

18.6.2	Show ONU light and port status .....	153
18.6.3	Configure MAC address aging time.....	153
18.6.4	Port maxMAC addresses .....	153
18.6.5	Show port MAC address table.....	153
18.6.6	Port isolate enable disable .....	154
18.6.7	Configure port negotiation mode .....	154
18.6.8	Show the port actually negotiation mode.....	154
18.6.9	Show port statistics .....	154
18.6.10	Configure port storm-control .....	155
18.6.11	WiFi configuration.....	155
18.6.12	SSID basic configuration.....	155
18.6.13	Configure WAN connection.....	157
18.6.14	Configure IGMP enable disable .....	158
18.6.15	Configure CATV management .....	158
18.6.16	Configure CTC OAM ignore.....	158
18.6.17	Configure reset to default.....	158
18.6.18	Configure clean the MAC table .....	159
18.6.19	Save the ONU configuration .....	159
18.7	Show/Remove onu configuration.....	159
18.8	ONU template management.....	160
18.8.1	Summary of the ONU template .....	160
18.8.2	DBA bandwidth template configuration.....	161
18.8.3	Services(SRV) template configuration.....	162
18.8.4	Alarm threshold template configuration .....	167
18.8.5	Auto bind template in PON port.....	170
18.8.6	Show/RemoveONU template configuration .....	171
19.	Controlling Switch Access with TACACS+ .....	172
19.1	Understanding TACACS+.....	172
19.2	TACACS+ Operation .....	173
19.3	Configuring TACACS+ .....	174
19.3.1	Default TACACS+ Configuration .....	174
19.3.2	Identifying the TACACS+ Server Host and Setting the Authentication Key.....	174
19.3.3	Configuring TACACS+ Login Authentication .....	175
19.3.4	Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services.....	177
19.3.5	Starting TACACS+ Accounting.....	177
19.4	Displaying the TACACS+ Configuration .....	178
20.	System Management .....	179
20.1	Configuration file management .....	179
20.1.1	Save configurations .....	179
20.1.2	Erase configurations .....	179
20.1.3	Show startup configurations.....	179
20.1.4	Show running configurations.....	179
20.1.5	Upload/download configuration file .....	179

20.2	Check the system information .....	180
20.2.1	Check system running information .....	180
20.2.2	Check version information .....	180
20.2.3	Check system running time.....	180
20.3	System basic configurations.....	181
20.3.1	Configure system name .....	181
20.3.2	Configure terminal display attribute.....	181
20.3.3	Configure terminal time-out value .....	181
20.4	System basic operations .....	181
20.4.1	Upgrade system.....	181
20.4.2	Network connectivity test .....	182
20.4.3	Reboot system.....	182
20.4.4	Telnet.....	182
20.4.5	Configure RTC system time .....	182
20.4.6	Fan control.....	183
20.5	OAM debug information .....	183
20.5.1	Enable/disable OAM debug information.....	183
20.5.2	Enable/disable CPU debug information .....	183
20.5.3	Enable/disable each function module debug information .....	184
21.	User Management.....	185
21.1	User privilege .....	185
21.2	Default user .....	185
21.3	Add user account .....	185
21.4	Show user account list .....	185
21.5	Delete user account .....	185
21.6	Modify password .....	186
22.	SNMP Configuration.....	187
22.1	SNMP introduction .....	187
22.2	SNMP version and MIB .....	187
22.3	Configure SNMP.....	188
22.3.1	Configure community.....	188
22.3.2	Configure Trap the target host address.....	188
22.3.3	Configure Administrator ID and contact method.....	189
22.3.4	Configure Ethernet switch location information .....	189
23.	Alarm and Event Management.....	190
23.1	Alarm and event introduction.....	190
23.2	Alarm management.....	190
23.2.1	System alarms.....	190
23.2.2	PON alarms.....	191
23.3	Event management.....	194
23.3.1	System events .....	194
23.3.2	PON events .....	194
23.3.3	ONU events.....	195
24.	OAM Interactive Information Management.....	196

---

23.1	Configure log output level of modules.....	196
23.2	Configure log store level of modules .....	196
25.	System Log .....	198
24.1	System log introduction .....	198
24.1.1	Log type.....	198
24.1.2	System log level.....	198
24.2	Configure system log .....	199
24.2.1	Show system log.....	199
24.2.2	Clear system log .....	199
24.2.3	Configure system log server .....	199
24.2.4	Configure save level of system log .....	199
24.2.5	Save system log to flash .....	200
24.2.6	Clear system log in flash.....	200
24.2.7	Upload system log .....	200

## 1. Access to OLT

### 1.1 Access to OLT CLI via console cable

GE PON OLT including 2/4/8 pon ports, total 3 models. You can access to OLT by CLI via console cable or telnet. This chapter introduces how to access to OLT CLI via console cable.

1. Connect PC to OLT console port by console cable.
2. Run hypertext terminal or other simulation tools such as secureCRT and Putty in PC. Set parameters as follows.

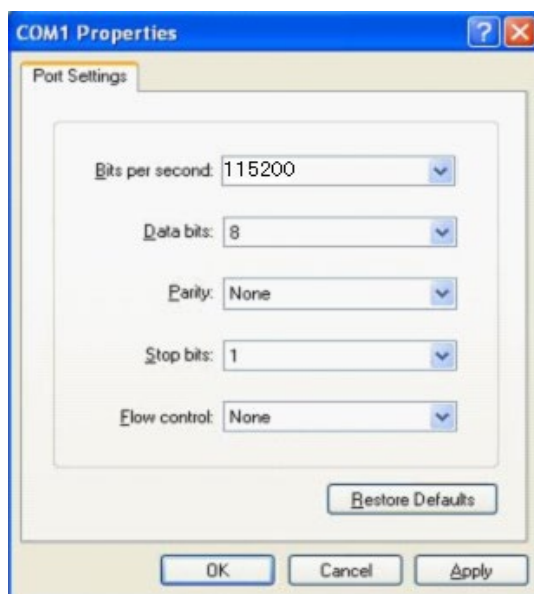
✧ Baudrate: **115200**

Data bits: **8**

✧ Parity: **none**

✧ Stop bits: **1**

✧ Follow control: **none**



COM port properties

After turned on the power, there is boot information printing. After startup, press enter and input username and password to login.

Notice:

*The default account is admin/Xpon@Olt9417#. For example,*

*Login: **admin***

*Password: **Xpon@Olt9417#***

*epon-olt> **enable***

*Password: **Xpon@Olt9417#***

*epon-olt#*

Input commands to configure or check device's status. Input "?" any time you need help.

This document will introduce each command Begin at next chapter.

## 1.2 Configuring the Switch for Secure Shell

This section describes how to configure the Secure Shell (SSH) feature.

### 1.2.1 Understanding SSH

SSH is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2).

#### 1.2.1.1 SSH Servers, Integrated Clients, and Supported Versions

The SSH feature has an SSH server and an SSH integrated client, which are applications that run on the switch. You can use an SSH client to connect to a switch running the SSH server.

The switch supports an SSHv1 or an SSHv2 server.

The switch supports an SSHv1 client.

SSH supports the Data Encryption Standard (DES) encryption algorithm, the Triple DES (3DES) encryption algorithm, and password-based user authentication.

SSH also supports these user authentication methods:

MAC address management includes:

- TACACS+ (for more information, see the "Controlling Switch Access with TACACS+" section)
- RADIUS
- Local authentication and authorization

#### 1.2.1.2 Limitations

These limitations apply to SSH:

- The switch supports Rivest, Shamir, and Adelman (RSA) authentication.
- SSH supports only the execution-shell application.
- The switch supports the Advanced Encryption Standard (AES) encryption algorithm

with a 128-bit key, 192-bit key, or 256-bit key. However, symmetric cipher AES to encrypt the keys is not supported.

## 1.2.2 Configuring SSH

### 1.2.2.1 Configuration Guidelines

Follow these guidelines when configuring the switch as an SSH server or SSH client:

- An RSA key pair generated by a SSHv1 server can be used by an SSHv2 server, and the reverse.
- If you get CLI error messages after entering the `crypto key generate rsa` global configuration command, an RSA key pair has not been generated. Reconfigure the hostname and domain, and then enter the `crypto key generate rsa` command. For more information, see the “Setting Up the Switch to Run SSH” section.
- When generating the RSA key pair, the message `No host name specified` might appear. If it does, you must configure a hostname by using the `hostname` global configuration command.
- When generating the RSA key pair, the message `No domain specified` might appear. If it does, you must configure an IP domain name by using the `ip domain-name` global configuration command.
- When configuring the local authentication and authorization authentication method, make sure that AAA is disabled on the console.

### 1.2.2.2 Setting Up the Switch to Run SSH

Follow these steps to set up your switch to run SSH:

1. Configure a hostname and IP domain name for the switch. Follow this procedure only if you are configuring the switch as an SSH server.
2. Generate an RSA key pair for the switch, which automatically enables SSH. Follow this procedure only if you are configuring the switch as an SSH server.
3. Configure user authentication for local or remote access. This step is required. For more information, see the “Configuring the Switch for Local Authentication and Authorization” section.

Begin at privileged configuration mode, follow these steps to configure a hostname and an IP domain name and to generate an RSA key pair. This procedure is required if you are configuring the switch as an SSH server.

	Command	Function
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>crypto key generate rsa usage-keys modulus &lt;1024-16384&gt;</code>	Enable the SSH server for local and remote authentication on the switch and generate an RSA key pair. We recommend that a minimum modulus size of 1024 bits. When you generate RSA keys, you are prompted

		to enter a modulus length. A longer modulus length might be more secure, but it takes longer to generate and to use.
<b>Step 3</b>	<b>show ip ssh</b>  <b>or</b>  <b>show ssh</b>	Show the version and configuration information for your SSH server.  Show the status of the SSH server on the switch.
<b>Step 4</b>	<b>copy running-config</b>  <b>startup-config</b>	(Optional) Save your entries in the configuration file.

To delete the RSA key pair, use the **crypto key zeroize rsa** global configuration command. After the RSA key pair is deleted, the SSH server is automatically disabled.

### 1.2.2.3 Configuring the SSH Server

Begin at privileged configuration mode, follow these steps to configure the SSH server:

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>ip ssh version [1   2]</b>	(Optional) Configure the switch to run SSH Version 1 or SSH Version 2. <ul style="list-style-type: none"> <li>• 1—Configure the switch to run SSH Version 1.</li> <li>• 2—Configure the switch to run SSH Version 2.</li> </ul> If you do not enter this command or do not specify a keyword, the SSH server selects the latest SSH version supported by the SSH client. For example, if the SSH client supports SSHv1 and SSHv2, the SSH server selects SSHv2.
<b>Step 3</b>	<b>ip ssh {timeout <i>seconds</i>   authentication-retries <i>number</i>}</b>	Configure the SSH control parameters: <ul style="list-style-type: none"> <li>• Specify the time-out value in seconds; the default is 120 seconds. The range is 0 to 120 seconds. This parameter applies to the SSH negotiation phase. After the connection is established, the switch uses the default time-out values of the CLI-based sessions.</li> </ul> By default, up to five simultaneous, encrypted SSH connections for multiple CLI-based sessions over the network are available (session 0 to session 4). After the execution shell starts, the

		<p>CLI-based session time-out value returns to the default of 10 minutes.</p> <ul style="list-style-type: none"> <li>Specify the number of times that a client can re-authenticate to the server. The default is 3; the range is 0 to 6.</li> </ul> <p>Repeat this step when configuring both parameters.</p>
<b>Step 4</b>	<p><b>show ip ssh</b></p> <p><b>or</b></p> <p><b>show ssh</b></p>	<p>Show the version and configuration information for your SSH server.</p> <p>Show the status of the SSH server on the switch.</p>
<b>Step 5</b>	<p><b>copy running-config</b></p> <p><b>startup-config</b></p>	<p>(Optional) Save your entries in the configuration file.</p>

To return to the default SSH control parameters, use the **no ip ssh {timeout | authentication-retries}** global configuration command.

### 1.2.3 Displaying the SSH Configuration and Status

To display the SSH server configuration and status, Use one or more of the following privileged EXEC commands.

<b>Command</b>	<b>Function</b>
<b>show ip ssh</b>	Shows the version and configuration information for the SSH server.
<b>show ssh</b>	Shows the status of the SSH server.

## 2. Command Line Interface

### 2.1 Abstract

GEPON OLT provides command line interface for configuration and management. The following is its specialities.

- Configure from console port.
- Input “?” any time you need help.
- Provide network test command, such as ping, for diagnosing connection.
- Provide FTP service for uploading and downloading files.
- Provide Doskey analogous function, you can execute a history command.
- Support ambiguous keywords searching, you just need to input unconflict keywords and press “tab” or “?”.

### 2.2 CLI configuration mode

GEPON OLT provides three configuration modes.

- Privileged mode
- Global configuration mode
- Interface configuration mode

The following table shows specialities, commands to enter and prompts.

CLI mode	Specialty	Prompt	Command to enter	Command to exit
Privileged mode	Show configurations and execute system commands	epon-olt#		<b>exit</b>
Global configuration mode	Configure system parameters	epon-olt(config)#	<b>configure terminal</b>	<b>exit</b>
Interface configuration mode	Configure interface parameters	epon-olt(config-if)#	<b>interface</b> <i>{interface_type slot/port}</i>	<b>exit</b>

### 2.3 CLI specialities

#### 1.2.4 Online help

GEPON OLT CLI provides the following online help:

- Completely help
- Partly help

You can get some help information of CLI with the help above.

(1) Input “?” to get all commands and illustrations at any configuration mode.

```
epon-olt(config)#
access-list      Add an access list entry.
banner          Set banner string
clean           Display system information.
copy            Copy configuration
debug           System debugging functions.
enable          Modify enable password parameters
  enable-password Set your enable password.
end             Exit current mode and down to previous mode
erase           Erase info from flash.
exec            exec system cmd
exit            Exit current mode and down to previous mode
fan             Specify olt fan management.
gateway         system manage gateway.
help            Description of the interactive help system
hostname        Set system's network name
igmp            Global IP configuration subcommands
interface       Select an interface to configure.
ip             IP information
ipmc            Global IP configuration subcommands
isolate         the isolate configuration information.Set switchport characteristics.
l3              set ecmp dip reg
line            Configure a terminal line
list            Print command list
log             Logging control
login-password  Reset your login password.
mac             Configure the MAC address table.
mc              pim add ipmc group
monitor         Configure SPAN monitoring.
no              Negate a command or set its default.
password        Assign the terminal connection password
pim             pim add ipmc group
ping            ping command
profile         Select profile to configure.
  queue-scheduler Configure egress queueing policy.
quit            Exit current mode and down to previous mode
reboot         Reboot the switch.
save            Display system information.
service         Set up miscellaneous service
set             Specify set command.
```

show	Show running system information.
snmp-server	Snmp server config
spanning-tree	Config STPD information.
storm-control	Specify the storm control.
switch	switch to shell
tftp	Specify tftp download.
time	Specify system time configuration.
upgrade	Specify upgrade system.
upload	Upload file for software or user config.
user	Manage System's users.
vlan	Vlan commands.
write	Write running configuration to memory, network, or terminal

- (2) Input “?” behind a command, it will display all key words and illustrations when this site should be a key word.

```
epon-olt(config)# interface
aux                aux interface.
gigabitethernet   Gigabitethernet IEEE 802.3.
gigabitethernet   GigabitEthernet IEEE 802.3z.
tengigabitethernet Ten GigabitEthernet interface.
vlan              Config vlan information.
```

- (3) Input “?” behind a command, it will display description of parameters when this site should be a parameter.

```
epon-olt(config)# access-list
<0-999>           IP standard access list.
<1000-1999>      IP extended access list.
<2000-2999>      L2 packet header access list.
<3000-3999>      User define field access list.
<4000-4999>      Vlan translation access list.
<5000-5999>      Port business access list.
<6000-6999>      Port quality of service access list.
<7000-7999>      Port Ipmc Vlan translation of service access list.
```

- (4) Input a character string end with “?”, it will display all key words that Begin at this character string.

```
epon-olt(config)# e
enable            Modify enable password parameters
enable-password   Set your enable password.
end              End current mode and change to enable mode.
erase            Erase info from flash.
exit            Exit current mode and down to previous mode
```

- (5) Input a command and a character string end with “?”, it will display all key words Begin at this character string.

```
epon-olt(config)# show ver
version          show version command.
```

- (6) Input a character string end with “Tab”, it will display completely key words that Begin at

this character string when it is unique.

### 1.2.5 Display specialities

GEPON OLT CLI provides the following display specialities. There is a pause when the information displays a whole screen at a time. Users have two ways to choose.

Operation	function
Input <Ctrl+C>	Stop displaying and executing.
Input any key	Continue displaying next screen

### 1.2.6 History commands

CLI provides Doskey analogous function. It can save history commands that executed before. Users can use direction key to invoke history command. The device can save at most ten commands.

Operation	action	result
Display history commands	<b>history</b>	Display all history commands.
Visit previous command	Up direction key “↑” or <Ctrl+P>	Display previous command if there is early history command.
Visit next command	Down direction key “↓” or <Ctrl+N>	Display next command if there is later history command.

### 1.2.7 Error messages

Every command will be executed if it passes syntax check. Otherwise it will come out error message. The following table shows some frequent errors.

Error messages	Reasons
Unknown command	No this command
	No this key word
	Parameter type error
	Parameter out of range
Command incomplete	Command is not complete
Too many parameters	Too many parameters
Ambiguous command	Command is ambiguous

### 1.2.8 Edit specialities

CLI provides basic edit function. Every command supports maxum 256 characters. The following table shows how to edit.

operation	function
Generally input	Insert character at cursor position and move cursor to right if edit buffer has enough space.
Backspace key	Delete the character in front of cursor.
Left direction key ← or <Ctrl+B>	Cursor moves one character position towards the left.

---

Right direction key → or <Ctrl+F>	Cursor moves one character position towards the right.
Up direction key ↑ or <Ctrl+P> Down direction key ↓ or <Ctrl+N>	Display history command.
Tab key	Input incomplete key words end with Tab key, CLI will provide partly help. If it is unique, the key word which matches what you input will be used and display in another row. If it should be parameter, or the key word is mismatched or matched but not unique, CLI will use what you input and display in another row.

## 3. Port Configuration

### 3.1 Port configuration

Port configuration mainly includes:

- enter port configuration mode
- enable or disable port
- configure port duplex mode
- configure port speed
- configure port VLAN mode
- configure port VLAN
- configure port PVID
- configure port flow control
- configure port broadcast suppression
- configure port multicast suppression
- configure port unknown unicast suppression
- configure port isolation
- configure port loopback
- configure port loopback detection

#### 3.1.1 Enter port configure mode

Begin at privileged configuration mode, input the following commands to enter port configuration mode.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> { <i>interface_type slot/port</i> }	Enter interface configuration mode.

#### 3.1.2 Enable /Disable port

You can use these commands to enable or disable port. The ports are enabled by default. If you want a port not to transfer data, you can shutdown it.

Begin at privileged configuration mode, enable or disable ports as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> { <i>interface_type slot/port</i> }	Enter interface configuration mode.
Step 3a	<b>no shutdown</b>	Enable port

Step 3b	<b>shutdown</b>	Disable port.
Step 4	<b>exit</b>	Exit to global configuration mode.
Step 5	<b>show interface</b> { <i>interface_type slot/port</i> }	Show interface configurations.
Step 6	<b>write</b>	Save configurations.

### 3.1.3 Configure port description

This command is used to configure port description. There is no description by default. Begin at privileged configuration mode, configure port description as the following table shows.

	<b>Command</b>	<b>Function</b>
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> { <i>interface_type slot/port</i> }	Enter interface configuration mode.
Step 3a	<b>description</b> < <i>string</i> >	Configure port description.
Step 3b	<b>no description</b>	Delete description.
Step 4	<b>exit</b>	Exit to global configuration mode.
Step 5	<b>show interface</b> { <i>interface_type slot/port</i> }	Show interface configurations.
Step 6	<b>write</b>	Save configurations.

### 3.1.4 Configure port duplex mode

Duplex includes full duplex and half duplex. When it works at full duplex, port can transmit and receive data at the same time; when it works at half duplex, port can only transmit or receive data at the same time. The duplex is auto by default.

Begin at privileged configuration mode, configure port duplex mode as the following table shows.

	<b>Command</b>	<b>Function</b>
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> { <i>interface_type slot/port</i> }	Enter interface configuration mode.
Step 3a	<b>duplex</b> { <b>auto</b>   <b>full</b>   <b>half</b> }	Configure port duplex mode.
Step 3b	<b>no duplex</b>	Reset duplex mode to default.
Step 4	<b>exit</b>	Exit to global configuration mode.
Step 5	<b>show interface</b> { <i>interface_type slot/port</i> }	Show interface configurations.
Step 6	<b>write</b>	Save configurations.

### 3.1.5 Configure port speed

When port speed mode is auto, the actual speed of port is determined by the automated negotiation result with opposite port. The speed is auto by default.

Begin at privileged configuration mode, configure port speed as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> { <i>interface_type slot/port</i> }	Enter interface configuration mode.
Step 3a	<b>speed</b> { 10   100   1000   auto }	Configure port speed.
Step 3b	<b>no speed</b>	Reset port speed to default.
Step 4	<b>exit</b>	Exit to global configuration mode.
Step 5	<b>show interface</b> { <i>interface_type slot/port</i> }	Show interface configurations.
Step 6	<b>write</b>	Save configurations.

### 3.1.6 Configure port rate limitation

Begin at privileged configuration mode, configure port rate limitation as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> { <i>interface_type slot/port</i> }	Enter interface configuration mode.
Step 3a	<b>line-rate</b> { <i>ingress   egress</i> } <b>bps</b> <i>value</i>	Configure port rate limitation. Value range: 64-1000000, it should be integral multiple of 64kbps.
Step 3b	<b>no line-rate</b> { <i>ingress   egress</i> }	Delete port rate limitation configurations.
Step 4	<b>exit</b>	Exit to global configuration mode.
Step 5	<b>show interface</b> { <i>interface_type slot/port</i> }	Show interface configurations.
Step 6	<b>write</b>	Save configurations.

### 3.1.7 Configure port VLAN mode

Each port has three VLAN mode, access, trunk and hybrid.

Access mode is usually used for port that connects with PC or other terminals, only one VLAN can be set up. Trunk mode is usually used for port that connects with switch; one or more VLAN can be set up. Hybrid mode can be used for port that connects with PC or switch. Default VLAN mode is hybrid.

Begin at privileged configuration mode, configure port VLAN mode as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface</b> <i>{interface_type slot/port}</i>	Enter interface configuration mode.
<b>Step 3a</b>	<b>switchport mode</b> { access   trunk   hybrid }	Configure port VLAN mode.
<b>Step 3b</b>	<b>no switchport mode</b>	Reset VLAN mode to default.
<b>Step 4</b>	<b>exit</b>	Exit to global configuration mode.
<b>Step 5</b>	<b>show interface</b> <i>{interface_type slot/port}</i>	Show interface configurations.
<b>Step 6</b>	<b>write</b>	Save configurations.

**Notice:**

All VLAN configurations will lose when you change port VLAN mode.

### 3.1.8 Configure hybrid port VLAN

Hybrid port can belong to several VLAN. It can be used to connect with switch or router, and also terminal host.

Begin at privileged configuration mode, configure hybrid port VLAN as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface</b> <i>{interface_type slot/port}</i>	Enter interface configuration mode.
<b>Step 3a</b>	<b>switchport hybrid vlan</b> <i>vlan_id</i> {tagged   untagged }	Add specific VLAN to hybrid port.
<b>Step 3b</b>	<b>switchport hybrid transparent</b>	Set port VLAN mode as transparent. OLT will add 1~4094 VLAN to the port. This operation will take about 3 minutes.
<b>Step 3c</b>	<b>no switchport hybrid vlan</b> <i>vlan_id</i>	Remove VLAN from port.
<b>Step 4</b>	<b>exit</b>	Exit to global configuration mode.
<b>Step 5</b>	<b>show interface</b> <i>{interface_type slot/port}</i>	Show interface configurations.
<b>Step 6</b>	<b>write</b>	Save configurations.

**Notice:**

You must configure PVID for the port that if it is configured untagged mode. PVID is the same as VLAN ID. Please refer to 3.1.10.

### 3.1.9 Configure trunk port VLAN

Trunk mode port can belong to several VLAN. It is usually used to connect with switches routers.

Begin at privileged configuration mode, configure trunk port VLAN as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration
Step 2	<b>interface</b> <i>{interface_type slot/port}</i>	Enter interface configuration
Step 3a	<b>switchport trunk vlan</b> <i>vlan_id</i>	Add specific VLAN to trunk port. VLAN mode is tagged.
Step 3b	<b>no switchport trunk vlan</b> <i>vlan_id</i>	Remove VLAN from port.
Step 5	<b>exit</b>	Exit to global configuration mode.
Step 6	<b>show interface</b> <i>{interface_type slot/port}</i>	Show interface configurations.
Step 7	<b>write</b>	Save configurations.

**Notice:**

If PVID of trunk mode port is the same as VLAN ID, the VLAN will add to the port as untagged mode.

### 3.1.10 Configure port PVID

Only under hybrid mode and trunk mode can set up PVID.

Begin at privileged configuration mode. Configure port PVID as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration.
Step 2	<b>interface</b> <i>{interface_type slot/port}</i>	Enter interface configuration mode.
Step 3a	<b>switchport</b> <i>{hybrid trunk}</i> <b>pvid</b> <i>vlan</i> <i>vlan_id</i>	Configure hybrid mode or trunk mode port PVID.
Step 3b	<b>no switchport</b> <i>{hybrid trunk}</i> <b>pvid</b>	Reset hybrid or trunk port PVID to default.
Step 4	<b>exit</b>	Exit to global configuration mode.
Step 5	<b>show interface</b> <i>{interface_type slot/port}</i>	Show interface configurations.
Step 6	<b>write</b>	Save configurations.

### 3.1.11 Configure access port VLAN

Only one untagged mode VLAN can be set to access port. Port's PVID is the same as VLAN ID.

Begin at privileged configuration mode, configure access port VLAN as the thable shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> { <i>interface_type slot/port</i> }	Enter interface configuration mode.
Step 3a	<b>switchportaccess vlan</b> <i>vlan_id</i>	Configure access port VLAN.
Step 3b	<b>no switchportaccess vlan</b>	Reset access port VLAN to default.
Step 4	<b>exit</b>	Exit to global configuration mode.
Step 5	<b>show interface</b> { <i>interface_type slot/port</i> }	Show interface configurations.
Step 6	<b>write</b>	Save configurations.

### 3.1.12 Configure port flow control

Begin at privileged configuration mode, configure port flow control as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> { <i>interface_type slot/port</i> }	Enter interface configuration mode.
Step 3a	<b>flowcontrol on</b>	Enable flow control function.
Step 3b	<b>no flowcontrol</b>	Disable flow control function.
Step 4	<b>exit</b>	Exit to global configuration mode.
Step 5	<b>show interface</b> { <i>interface_type slot/port</i> }	Show interface configurations.
Step 6	<b>write</b>	Save configurations.

### 3.1.13 Configure port broadcast suppression

Begin at privileged configuration mode, configure port broadcast suppression as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> { <i>interface_type slot/port</i> }	Enter interface configuration mode.
Step 3a	<b>storm-control broadcast pps</b> <i>value</i>	Configure broadcast suppression. Value range: 64-1000000, it should be integral multiple of 64kbps.

<b>Step 3b</b>	<b>no storm-control broadcast</b>	Remove broadcast suppression.
<b>Step 4</b>	<b>exit</b>	Exit global configuration mode.
<b>Step 5</b>	<b>show interface</b> { <i>interface_type slot/port</i> }	Show interface configurations.
<b>Step 6</b>	<b>write</b>	Save configurations.

### 3.1.14 Configure port multicast suppression

Begin at privileged configuration mode, configure port multicast suppression as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface</b> { <i>interface_type slot/port</i> }	Enter interface configuration mode.
<b>Step 3a</b>	<b>storm-control multicast ppsvalue</b>	Configure multicast suppression. Value range: 64-1000000, it should be integral multiple of 64kbps.
<b>Step 3b</b>	<b>no storm-control multicast</b>	Remove multicast suppression.
<b>Step 4</b>	<b>exit</b>	Exit global configuration mode.
<b>Step 5</b>	<b>show interface</b> { <i>interface_type slot/port</i> }	Show interface configurations.
<b>Step 6</b>	<b>write</b>	Save configurations.

### 3.1.15 Configure port unknown unicast suppression

Begin at privileged configuration mode, configure port unknown unicast suppression as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface</b> { <i>interface_type slot/port</i> }	Enter interface configuration mode.
<b>Step 3a</b>	<b>storm-control unicast ppsvalue</b>	Configure unknown unicast suppression. Value range: 64-1000000, it should be integral multiple of 64kbps.
<b>Step 3b</b>	<b>no storm-control unicast</b>	Remove unknown unicast suppression.

<b>Step 4</b>	<b>exit</b>	Exit global configuration mode.
<b>Step 5</b>	<b>show interface</b> <i>{interface_type slot/port}</i>	Show interface configurations.
<b>Step 6</b>	<b>write</b>	Save configurations.

### 3.1.16 Configure port isolation

With this function, customers can add ports to a same isolation group so that these ports can be isolated among L2 and L3 steams. This will improve security of network and provide flexible networking scheme.

Begin at privileged configuration mode, configure port isolation as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface</b> <i>{interface_type slot/port}</i>	Enter interface configuration mode.
<b>Step 3a</b>	<b>switchport isolate</b>	Add port to isolation group.
<b>Step 3b</b>	<b>no switchport isolate</b>	Remove port from isolation group.
<b>Step 4</b>	<b>exit</b>	Exit to global configuration mode.
<b>Step 5a</b>	<b>show interface</b> <i>{interface_type slot/port}</i>	Show interface configurations.
<b>Step 5b</b>	<b>show isolate port</b>	Show isolation group.
<b>Step 6</b>	<b>write</b>	Save configurations.

### 3.1.17 Configure port loopback

Begin at privileged configuration mode, configure port loopback as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface</b> <i>{interface_type slot/port}</i>	Enter interface configuration mode.
<b>Step 3</b>	<b>loopback</b> [internal   external   outside]	Internal means cpu inner loopback. External means cpu outer loopback. Outside means external data loopback.
<b>Step 4</b>	<b>exit</b>	Exit to global configuration mode.

**Notice:**

When testing port loopback function, please disable port loopback detection. Please refer to 3.1.18.

### 3.1.18 Configure port loopback detection

Begin at privileged configuration mode, configure port loopback detection as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2a</b>	<b>loopback detect enable</b>	Enable port loopback detection.
<b>Step 2b</b>	<b>no loopback detect</b>	Disable port loopback detection.
<b>Step 3</b>	<b>show loopback detect</b>	Show port loopback detection status.
<b>Step 4</b>	<b>exit</b>	Exit to global configuration mode.

### 3.1.19 Configure port jumboframe

Begin at privileged configuration mode, configure jumboframe that the port can pass as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface {interface_type slot/port}</b>	Enter interface configuration mode.
<b>Step 3a</b>	<b>jumboframe enable</b>	Enable jumboframe transmission. By default, switch chipset supports transmitting maximum 1536 bytes frame; PON chipset supports transmitting maximum 2047 bytes frame.
<b>Step 3b</b>	<b>no jumboframe</b>	Disable jumboframe transmission.
<b>Step 4</b>	<b>exit</b>	Exit to global configuration mode.

### 3.1.20 Show port statistics

Begin at privileged configuration mode, show port statistics as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface {interface_type slot/port}</b>	Enter interface configuration mode.

<b>Step 3</b>	<b>show statistics</b>	Show port statistics.
<b>Step 4</b>	<b>exit</b>	Exit to global configuration mode.

### 3.1.21 Clean port statistics

Begin at privileged configuration mode, clean port statistics as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>show interface</b> <i>{interface_type slot/port}</i>	Show port statistics.
<b>Step 3</b>	<b>clean statistics</b>	Clean port statistics.

### 3.1.22 Show interface configurations

Operation	Command
Show interface configurations.	<b>Show interface</b> <i>{interface_type slot/port}</i>

In the system, interface gigabitEthernet 0/1~0/x stands for uplink port 1~x. Interface epon0/1~0/x stands for EPON port 1~x.

For example, display configurations of uplink port 5.

```
epon-olt(config)# show interface gigabitEthernet 0/5
```

Interface gigabitEthernet0/5's information.

GigabitEthernet0/5 current state : Down

Hardware Type is Gigabit Ethernet, Hardware address is 0:0:0:0:0:0

The Maximum Transmit Unit is 1500

Media type is twisted pair, loopback not set

Port hardware type is 1000Base-TX

Link speed type: autonegotiation, Link duplex type: autonegotiation

Current link state: Down

Current autonegotiation mode: enable

Current link speed: 1000Mbps, Current link mode: half-duplex

Flow Control: disable MDIX Mode: force

The Maximum Frame Length is 1536

Broadcast storm control: 512 fps

Multicast storm control: disable

Unknown unicast storm control: 512 fps

Ingress line rate control: no limit

Egress line rate control: no limit

mac address learn state : enable, no limit

Port priority: 0

PVID: 1

Port combo mode: null

```

Isolate member : yes
  Port link-type: hybrid
  Untagged VLAN ID: 1
  Tagged VLAN ID : 100
  Last 300 seconds input: 0 packets 0 bytes
  Last 300 seconds output: 0 packets 0 bytes
Input(total): 1113473691 packets, 4081075466 bytes
              0 broadcasts, 1113473687 multicasts
Input(normal): 1113473691 packets, 4081075466 bytes
              0 broadcasts, 1113473687 multicasts, 0 pauses
Input: 0 input errors, 0 runts, 0 giants, 0 throttles, 4 CRC
      0 overruns, 0 aborts, 0 ignored, 0 parity errors
Output(total): 4371 packets, 351860 bytes
              1280 broadcasts, 3091 multicasts, 0 pauses
Output(normal): 4371 packets, 351860 bytes
              1280 broadcasts, 3091 multicasts, 0 pauses
Output: 0 output errors, 0 underruns, 0 buffer failures
      0 aborts, 0 deferred, 0 collisions, 0 late collisions
      0 lost carrier, 0 no carrier

```

### 3.1.23 Set to 10G mode

Begin at privileged configuration mode, set to 10G mode as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>debug mode</b>	Enter debug mode.
<b>Step 3</b>	<b>set giu mode sfp+</b>	Set to 10G mode.
<b>Step 4</b>	<b>exit</b>	Exit to global configuration mode.
<b>Step 5</b>	<b>reboot</b>	Reboot olt to take effect.

## 3.2 Example

Configure VLAN and broadcast suppression of trunk mode port.

### 1. Requirement

Uplink port 1 of OLT connects to switch, port mode is trunk. It can pass through VLAN 20 and VLAN 100, add VLAN tag 123 to untagged streams. Rate of broadcast streams is 64bps.

### 2. Framework



### 3. Steps

(1) Enter interface configuration mode.

```
epon-olt(config)# interface gigabitethernet 0/1
```

```
epon-olt(config-if-ge0/1) #
```

(2) Configure port mode and add VLAN

```
epon-olt(config-if-ge0/1) # switchport mode trunk
```

```
epon-olt(config-if-ge0/1) # switchport trunk vlan 20
```

```
epon-olt(config-if-ge0/1) # switchport trunk vlan 100
```

PS. The VLAN must be added first. Please refer to 4.1.1.

(3) Configure port PVID

```
epon-olt(config-if-ge0/1) # switchport trunk pvid vlan 123
```

(4) Configure port broadcast suppression

```
epon-olt(config-if-ge0/1) # storm-control broadcast bps 64
```

## 4. Port Aggregation Configuration

### 4.1 Introduction

Port aggregation is that several ports constitute an aggregation group so that it can share responsibility for traffic load in each port. When one link is broken down, the traffic will switch to another automatically to ensure traffic is unblocked. It seems that the aggregation group is the same as a port.

In an aggregation group, member ports must have the same speed, the same duplex mode and the same basic configurations. Basic configurations contain:

- (1) STP configurations such as STP status, link properties (e.g. p2p port), priority, cost, message format, loopdetect status, edge port or not.
- (2) QoS configurations such as rate limiting, priority mark, 802.1p priority, congestion avoidance.
- (3) VLAN configurations such as VLAN ID, PVID.
- (4) Port link type such as trunk mode, hybrid mode and access mode.
- (5) GVRP configurations such as switch status, registration type, timer value.

### 4.2 Port Aggregation Configuration

#### 4.2.1 Create static aggregation group

At most 4 groups can be created. You can add 4 member ports altogether in every group and at most 4 ports will come into being aggregation at the same time.

Every group is defined as a channel group; the commands are centre on channel group.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2a</b>	<b>channel-group &lt;1-4&gt; mode static</b>	Create static aggregation group.
<b>Step 2b</b>	<b>no channel-group &lt;1-4&gt;</b>	Delete static aggregation group.
<b>Step 3</b>	<b>show channel-group summary</b>	Show static aggregation group configuration.

#### 4.2.2 Configure load balancing policy of aggregation group

Configuring load balancing policy includes source MAC, destination MAC, both source and destination MAC, source IP, destination IP, both source and destination IP. Default load balancing policy is based on source MAC.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>channel-group &lt;1-4&gt; load-balance {smac dmac sdlmac sip dip sdip}</b>	Specify which link is used to transmit traffic in aggregation group.
<b>Step 3</b>	<b>show channel-group summary</b>	Show aggregation configurations.

#### 4.2.3 Configure member port of aggregation group

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface {interface_type slot/port}</b>	Enter interface configuration mode.
<b>Step 3a</b>	<b>channel-group &lt;1-4&gt;</b>	Add current port to specific channel group.
<b>Step 3b</b>	<b>no channel-group &lt;1-4&gt;</b>	Delete current port from specific channel group.
<b>Step 4</b>	<b>exit</b>	Exit global configuration mode.
<b>Step 5</b>	<b>show channel-group summary</b>	Show aggregation group configurations.

## 5. VLAN Configuration

### 5.1 VLAN configuration

VLAN configuration mainly contains:

- Create/delete VLAN
- Configure/delete VLAN description
- Configure/delete IP address and mask of VLAN

#### 5.1.1 Create/Delete VLAN

Begin at privileged configuration mode, create or delete VLAN as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2a</b>	<b>vlan</b> <i>vlan_id</i>	Create VLAN or enter VLAN interface configuration mode. VLAN ID range is from 1 to 4094.
<b>Step 2b</b>	<b>no vlan</b> <i>vlan_id</i>	Delete specific VLAN.
<b>Step 3</b>	<b>exit</b>	Exit to global configuration mode.
<b>Step 4a</b>	<b>show vlan</b> [ <i>vlan_id/all</i> ]	Show VLAN configurations. Choosing <b>all</b> means display all existed VLAN. And choosing <i>vlan_id</i> means display information of specific VLAN.
<b>Step 4b</b>	<b>show vlan</b>	Show information of all existed VLAN.
<b>Step 5</b>	<b>write</b>	Save configurations.

#### 5.1.2 Configure/delete VLAN description

Begin at privileged configuration mode, configure or delete VLAN description as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface vlan</b> <i>vlan_id</i>	Create VLAN or enter VLAN interface configuration mode. VLAN ID range is from 1 to 4094.

<b>Step 3a</b>	<b>description</b> <i>string</i>	Configure VLAN description.
<b>Step 3b</b>	<b>no description</b>	Delete VLAN description.
<b>Step 4</b>	<b>exit</b>	Exit to global configuration mode.
<b>Step 5</b>	<b>show interface vlan</b> <i>vlan_id</i>	Show VLAN interface information.
<b>Step 6</b>	<b>write</b>	Save configurations.

**Notice:**

By default, VLAN description is VLAN ID, such as “vlan 1”.

### 5.1.3 Configure/delete IP address and mask of VLAN

Begin at privileged configuration mode, configure or delete IP address and mask of VLAN as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>config terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface vlan</b> <i>vlan_id</i>	Enter VLAN interface configuration mode. VLAN ID range is from 1 to 4094.
<b>Step 3a</b>	<b>ipaddress</b> < <i>A.B.C.D</i> > <i>net-mask</i>	Configure IP address and mask of VLAN.
<b>Step 3b</b>	<b>no ipaddress</b> < <i>A.B.C.D</i> >	Delete IP address and mask of VLAN.
<b>Step 4</b>	<b>exit</b>	Exit to global configuration mode.
<b>Step 5</b>	<b>show interface vlan</b> <i>vlan_id</i>	Show VLAN information.
<b>Step 6</b>	<b>write</b>	Save configurations.

## 5.2 Show VLAN information

Input the following commands to Show VLAN information and port members.

<b>Operation</b>	<b>Command</b>
Show VLAN information	<b>show interface vlan</b>
Show VLAN port members	<b>show interface vlan</b> <i>vlan-id</i>

**Example:**

```
Show VLAN 100 port members
epon-olt(config)# show in vlan 100
Vlan ID      : 100
```

Name : vlan100  
Mac address : 00:90:4c:06:a5:73  
Tagged Ports : ge0/4 ge0/5  
epon0/1  
Untagged Ports : ge0/8

## 6. VLAN Translation/QinQ

### 6.1 Configure VLAN translation/QinQ

Begin at privileged configuration mode, configure VLAN translation/QinQ as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> { <i>interface_type slot/port</i> }	Enter interface configuration mode.
Step 3a	<b>dot1q-tunnelvlan-mapping</b> <i>ori_vlan</i> { <i>any ori_vlan_pri</i> } <i>tra_vlani</i> { <i>any tra_vlan_pri</i> } { <b>db-tag one-tag</b> }	Configure VLAN translation/QinQ. db-tag means QinQ. one-tag means translation.
Step 3b	<b>no</b> <b>dot1q-tunnelvlan-mapping</b> <i>ori_vlantra_v</i> <i>lanid</i>	Delete VLAN translation/QinQ.
Step 4	<b>exit</b>	Exit to global configuration mode.
Step 5	<b>show vlanvlan-mapping interface</b> { <i>interface_type slot/port</i> }	Show VLAN translation/QinQ configurations.
Step 6	<b>write</b>	Save configurations.

### 6.2 Example

#### (1)VLAN translation function

Configure GE1 VLAN translation function, CVLAN is 100, priority is 1, and translated VLAN is 200, priority is 2.

```
epon-olt(config)# interface gigabitethernet 0/1
epon-olt(config-if)#switchport hybrid vlan 100 tagged
epon-olt(config-if)#switchport hybrid vlan 200 tagged
epon-olt(config-if)# dot1q-tunnel vlan-mapping 100 1 200 2 one-tagged
epon-olt(config)#show vlan vlan-mapping interface gigabitethernet 0/1
```

#### (2)QinQ function

Configure GE2 QinQ function, CVLAN is 300, priority is 3, and SVLAN is 400, priority is 4.

```
epon-olt(config)# interface gigabitethernet 0/2
epon-olt(config-if)#switchport hybrid vlan 300 tagged
epon-olt(config-if)#switchport hybrid vlan 400 tagged
epon-olt(config-if)# dot1q-tunnel vlan-mapping 300 3 400 4 db-tagged
```

```
epon-olt(config)#show vlan vlan-mapping interface gigabitethernet 0/2
```

## 7. MAC Address Configuration

### 7.1 Overview

In order to forward messages rapidly, a device need to maintain its MAC address table. MAC address table contains MAC addresses that connect with the device, ports, VLAN, type and aging status. Dynamic MAC addresses in the table are learnt by device. The process of learning is that: if port A receives a message, device will analyze the source MAC address (SrcMAC), and think of messages whose destination MAC address is SrcMAC can be forwarded to port A. If SrcMAC has been in the table, device will update it; if not, device will add this new address to the table.

For the messages whose destination MAC address can be found in MAC address table, they are forwarded by hardware. Otherwise, they flood to all ports. When flooded messages arrive to its destination, the destination device will respond. The device will add new MAC to the table. Then, messages with this destination MAC will be forwarded via the new table. However, when messages still can't find its destination by flood, device will discard them and tell sender destination is unreachable.

### 7.2 Configure MAC address

MAC address management includes:

- Configure MAC address table
- Configure MAC address aging time

#### 7.2.1 Configure MAC address table

You can add static MAC address entries, delete MAC address entries or clean MAC address table.

Begin at privileged configuration mode, configure MAC address table as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2a</b>	<b>mac address-table static vlan</b> <i>vlan_idxxx:xxx:xxx interface</i> <i>interface_type slot/port</i>	Add static MAC address entry.
<b>Step 2b</b>	<b>no mac address-table vlan</b> <i>vlan_id</i> <i>xxx:xxx:xxx</i>	Delete MAC address entry.
<b>Step 2c</b>	<b>mac address-table clean</b>	Clean MAC address table.

<b>Step 3</b>	<b>show mac address-table</b>	Show MAC address table.
<b>Step 4</b>	<b>write</b>	Save configurations.

### 7.2.2 Configure MAC address aging time

There is aging time in device. If device doesn't receive any message from other devices in aging time, it will delete the MAC address from MAC table. But for static MAC in the table, aging time is not effective.

Begin at privileged configuration mode, configure MAC address aging time as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>mac address-table agingtime <i>value</i></b>	Configure MAC address aging time, range is 10-1000000s. 0s means don't aging. Default is 300s.
<b>Step 3</b>	<b>show mac address-table agingtime</b>	Show aging time.
<b>Step 4</b>	<b>write</b>	Save configurations.

### 7.2.3 Clean MAC address table

Begin at privileged configuration mode, clean MAC address table as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>mac address-table clean</b>	Clean MAC address table.

### 7.2.4 Configure maximum learnt MAC entries of port

Begin at privileged configuration mode, configure maximum learnt MAC entries of port as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface <i>{interface_type slot/port}</i></b>	Enter interface configuration mode.
<b>Step 3</b>	<b>mac-address mac-limit&lt;0-16384&gt;</b>	0 means no limitation.
<b>Step 4</b>	<b>exit</b>	Exit to global configuration mode.

## 7.3 Show MAC address table

### 7.3.1 Show MAC address table

Begin at privileged configuration mode, show MAC address table as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2a</b>	<b>show mac address-table</b> <b>interface</b> { <i>interface_type slot/port</i> }	Show MAC address table based on Ethernet port.
<b>Step 2b</b>	<b>show mac address-table vlan</b> <i>vlan_id</i>	Show MAC address table based on VLAN ID.
<b>Step 2c</b>	<b>show mac address-table</b>	Show whole MAC address table.
<b>Step 2d</b>	<b>interface</b> { <i>interface_type slot/port</i> }	Enter the PON port
<b>Step 3</b>	<b>show pon mac-address-table</b>	Show pon port MAC address table

### 7.3.2 Show MAC address aging time

Begin at privileged configuration mode, show MAC address aging time as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>show mac address-table agingtime</b>	Show MAC address aging time.

## 7.4 Configure MAC flapping

MAC flapping includes:

- Configure MAC flapping status
- Configure MAC flapping interval
- Configure MAC flapping mode
- Configure MAC flapping range
- Configure MAC flapping suppression
- Configuring MAC flapping port status
- Clear MAC flapping Table

### 7.4.1 Configure MAC flapping status

Begin at privileged configuration mode, configure MAC flapping status as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>mac address-table mac-flapping</b>	Enable MAC flapping.
<b>Step 3</b>	<b>write</b>	Save configurations.

To close MAC flapping, use the **no mac address-table mac-flapping** global configuration command.

#### 7.4.2 Configure MAC flapping interval

Begin at privileged configuration mode, configure MAC address flapping interval as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>mac address-table mac-flapping interval</b> <i>&lt;10-3600&gt;</i>	Configure MAC address flapping interval.
<b>Step 3</b>	<b>show mac address-table mac-flapping</b>	Show mac flapping table .
<b>Step 4</b>	<b>write</b>	Save configurations.

#### 7.4.3 Configure MAC flapping Mode

Begin at privileged configuration mode, configure MAC address flapping mode as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>mac address-table mac-flapping mode</b> <i>[only-alarm auto-recovery manual-recovery]</i>	Configure MAC address flapping Mode.
<b>Step 3</b>	<b>show mac address-table mac-flapping</b>	Show mac flapping table.
<b>Step 4</b>	<b>write</b>	Save configurations.

#### 7.4.4 Configure MAC flapping Range

Begin at privileged configuration mode, configure MAC flapping range as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>mac address-table mac-flapping range</b> <i>[uplink pon all]</i>	Configure MAC flapping range.

Step 3	<b>show mac address-table mac-flapping suppression</b>	Show mac flapping table.
Step 4	<b>write</b>	Save configurations.

#### 7.4.5 Configure MAC flapping suppression

Begin at privileged configuration mode, configure MAC flapping suppression as the following table shows.

	<b>Command</b>	<b>Function</b>
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2a	<b>mac address-table mac-flapping suppression threshold &lt;1-256&gt;</b>	Configure MAC flapping suppression threshold.
Step 2b	<b>mac address-table mac-flapping suppression aging-time &lt;10-3600&gt;</b>	Configure MAC flapping suppression aging-time.
Step 3	<b>show mac address-table mac-flapping suppression</b>	Show mac flapping table.
Step 4	<b>write</b>	Save configurations.

#### 7.4.6 Configuring MAC flapping port status

Begin at privileged configuration mode, configure MAC flapping port status as the following table shows.

	<b>Command</b>	<b>Function</b>
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface <i>interface_type slot/port</i></b>	Enter interface configuration mode, and specify the interface to be configured.
Step 3	<b>mac address-table mac-flapping [enable disable]</b>	Configuring MAC flapping port status.
Step 4	<b>show mac address-table mac-flapping suppression</b>	Show mac flapping table.
Step 5	<b>write</b>	Save configurations.

#### 7.4.7 Clear MAC flapping Table

Begin at privileged configuration mode, the steps to clear MAC flapping Table as the following table shows.

	<b>Command</b>	<b>Function</b>
Step 1	<b>configure terminal</b>	Enter global configuration

		mode.
<b>Step 2</b>	<b>mac address-table mac-flapping clear</b>	Clear MAC flapping Table.

## 7.5 Show MAC flapping

### 7.5.1 Show MAC flapping information

Begin at privileged configuration mode, show MAC flapping information table as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>show mac address-table mac-flapping</b>	Show MAC flapping information table.

### 7.5.2 Show MAC flapping port status

Begin at privileged configuration mode, show MAC flapping configuration as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>show mac address-table mac-flapping suppression</b>	Show MAC flapping suppression configuration.
<b>Step 3</b>	<b>show mac address-table mac-flapping port</b>	Show the port status.

## 8. Configure Port Mirroring

Port mirroring is to copy one or more ports' traffic to specific port. It is usually used for network traffic analysis and diagnosis.

The device supports 4 mirroring sessions.

### 8.1 Configure mirroring destination port

Begin at privileged configuration mode, configure mirroring destination port as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>monitor session <i>session_number</i> destination interface <i>interface_type</i> <i>interface_num</i></b>	Configure mirroring destination port. Session number is 1~4.
<b>Step 3</b>	<b>show monitor session all</b>	Show mirroring configurations.
<b>Step 4</b>	<b>write</b>	Save configurations.

### 8.2 Configure mirroring source port

Mirroring source port is the port we want to monitor. Data that pass through the port will be copied to mirroring destination port.

Begin at privileged configuration mode, configure mirroring source port as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>monitor session <i>session_number</i> source interface <i>interface_type</i> <i>start_interface_num</i> [ - <i>end_interface_num</i> ] {<b>both</b> <b>rx</b> <b>tx</b>}</b>	Configure mirroring source port. session_number is 1-4. <b>Both</b> means received data and transmitted data. <b>rx</b> means received data. <b>tx</b> means transmitted data.
<b>Step 3</b>	<b>show monitor session all</b>	Show mirroring configurations.
<b>Step 4</b>	<b>write</b>	Save configurations.

### 8.3 Delete port mirroring

Begin at privileged configuration mode, delete port mirroring as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>no monitor session</b> <i>session_number</i> { <b>[destination   source]</b> <b>interface</b> <i>interface_type</i> <i>slot/port</i> }	Delete port mirroring. <i>session_number</i> is 1-4
<b>Step 3</b>	<b>show monitor session all</b>	Show mirroring configurations.

**Example:**

Mirror data from epon 0/1 to uplink port 1.

```
epon-olt(config)# monitor session 1 destination interface gigabitethernet 0/1
```

```
epon-olt(config)# monitor session 1 source interface epon0/1 both
```

## 9. IGMP Configuration

### 9.1 IGMP Snooping

#### 9.1.1 Enable/disable IGMP Snooping

IGMP snooping is disabled by default. You should enable by the following command. Begin at privileged configuration mode, enable/disable IGMP snooping as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2a	<b>ip igmpsnoothing enable</b>	Enable IGMP Snooping.
Step 2b	<b>no ip igmp snooping</b>	Disable IGMP snooping.
Step 3	<b>show ip igmpsnoothing configuration</b>	Show IGMP snooping configurations.
Step 4	<b>write</b>	Save configurations.

#### 9.1.2 Configure multicast data forwarding mode

Begin at privileged configuration mode, configure multicast data forwarding mode as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ip igmp snooping forward vlan <i>vlan-id</i> mode { flood   forward   strict-forward }</b>	Configure multicast data forwarding mode.
Step 3	<b>write</b>	Save configurations.

#### 9.1.3 Configure port multicast VLAN

After add VLAN to the port, you should also configure multicast VLAN for multicast service. Begin at privileged configuration mode, configure port multicast VLAN as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface{<i>interface_type slot/port</i>}</b>	Enter interface configuration mode.

Step 3a	<b>ip igmp snooping user-vlan vlan_id group-vlan vlan_id { tagged   untagged }</b>	Configure port multicast VLAN. VLAN range is 1-4094.
Step 3b	<b>no ip igmp snooping group-vlan vlan_id</b>	Delete port multicast VLAN.
Step 4	<b>exit</b>	Exit to global configuration mode.
Step 5	<b>show ip igmpsnooping user-vlan</b>	Show multicast VLAN.
Step 6	<b>write</b>	Save configurations.

#### 9.1.4 Configure multicast router port

Multicast router port is used to forward IGMP messages. Usually, uplink port is configured as multicast router port.

Begin at privileged configuration mode, configure multicast router port as the following table shows.

	<b>Command</b>	<b>Function</b>
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2a	<b>ip igmpsnooping mrouter vlan vlan-id interface {interface_type slot/port}</b>	Configure multicast router port.
Step 2b	<b>no ip igmpsnooping mrouter vlan vlan-id interface {interface_type slot/port}</b>	Delete multicast router port.
Step 3	<b>show ip igmp-snooping mrouter vlan all</b>	Show multicast router mode configuration.
Step 4	<b>write</b>	Save configurations.

#### 9.1.5 Configure static multicast

Begin at privileged configuration mode, configure static multicast as the following table shows.

	<b>Command</b>	<b>Function</b>
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2a	<b>ip igmpsnooping static vlan vlan-id&lt;A.B.C.D&gt; interface interface-id</b>	Configure static multicast.
Step 2b	<b>no ip igmpsnooping static vlan vlan-id&lt;A.B.C.D&gt; interface {interface_type slot/port}</b>	Delete static multicast.
Step 3	<b>show ip igmp-snooping configuration</b>	Show IGMP configurations.
Step 4	<b>write</b>	Save configurations.

#### 9.1.6 Configure fast leave

Begin at privileged configuration mode, configure fast leave as the following table shows.

	<b>Command</b>	<b>Function</b>
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> { <i>interface_type slot/port</i> }	Enter interface configuration mode.
Step 3a	<b>ip igmpsnooping immediate-leave</b>	Enable fast leave.
Step 3b	<b>no ip igmpsnooping immediate-leave</b>	Disable fast leave.
Step 4	<b>exit</b>	Exit to global configuration mode.
Step 5	<b>show ip igmp snooping port information</b>	Show port IGMP information.
Step 6	<b>write</b>	Save configurations.

### 9.1.7 Configure multicast group limit

Begin at privileged configuration mode, configure multicast group limitation as the following table shows.

	<b>Command</b>	<b>Function</b>
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> { <i>interface_type slot/port</i> }	Enter interface configuration mode.
Step 3a	<b>ip igmpsnooping limit</b> <0-1024>	Configure port multicast group limitation.
Step 3b	<b>no ip igmpsnooping limit</b>	Reset multicast group limitation to default.
Step 4	<b>exit</b>	Exit to global configuration mode.
Step 5	<b>show ip igmp snooping port information</b>	Show port multicast information.
Step 6	<b>write</b>	Save configurations.

### 9.1.8 Configure parameters of special query

Begin at privileged configuration mode, configure parameters of specific query as the following table shows.

	<b>Command</b>	<b>Function</b>
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2a	<b>ip igmp snooping lastmember-querycount</b> <1-255>	Configure specific query count. Default is 2.
Step 2b	<b>ip igmp snooping lastmember-queryinterval</b> <1-255	Configure specific query interval. Default is 1s.

	>	
Step 2c	<b>ip igmp snooping lastmember-query response</b> <1-255>	Configure specific query response time. Default is 1s.
	>	
Step 3	<b>show ip igmp snooping configuration</b>	Show IGMP configurations.
Step 4	<b>write</b>	Save configurations.

### 9.1.9 Configure parameters of general query

Begin at privileged configuration mode, configure parameters of general query as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2a	<b>ip igmp snooping general-query-packet</b> <enable disable>	Enable or disable general query function. Default is disable.
Step 2b	<b>ip igmp snooping general-query-time</b> <10-255>	Configure general query interval. Default is 126s.
Step 3	<b>show ip igmp snooping configuration</b>	Show IGMP configurations.
Step 4	<b>write</b>	Save configurations.

### 9.1.10 Configure source IP of query

Begin at privileged configuration mode, configure source IP of query message as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ip igmp snooping member-query source-ip</b> <A.B.C.D>	Configure source IP of query message. Default is 1.1.1.1.
Step 3	<b>show ip igmp snooping configuration</b>	Show IGMP configurations.
Step 4	<b>write</b>	Save configurations.

### 9.1.11 Configure multicast member aging time

If the port doesn't receive any report message from member in aging time, device will delete this port from group members.

Begin at privileged configuration mode, configure multicast member aging time as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.

<b>Step 2</b>	<b>ip igmpsnooping host-aging-timevalue</b>	Configure multicast port member aging time. Value range is 10-3600s, default is 260s.
<b>Step 3</b>	<b>show ip igmpsnooping configuration</b>	Show IGMP configurations.
<b>Step 4</b>	<b>write</b>	Save configurations.

### 9.1.12 Show multicast group information

If there is a member join a group, you can use the following commands to show multicast group information.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2a</b>	<b>show ip igmpsnooping vlan [vlan-id   all]</b>	Show multicast group information.
<b>Step 2b</b>	<b>show ip igmp snooping statistic</b>	Show multicast statistic.

## 9.2 Example

This example introduces how to configure IGMP snooping function, including multicast VLAN, multicast router port and ONU LAN port, etc.

### 1. Requirement

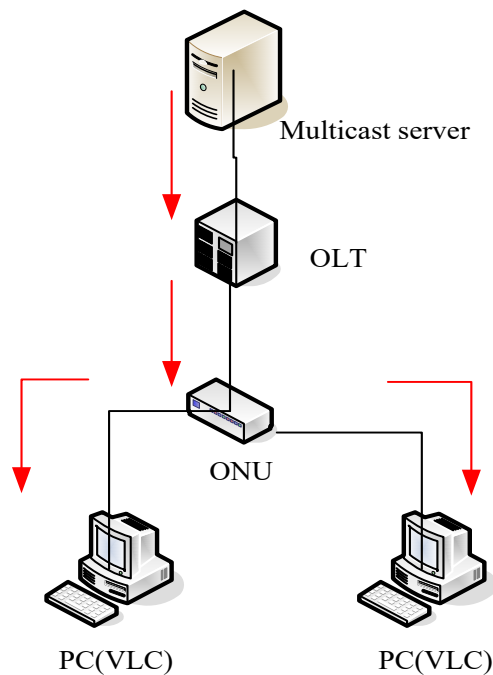
In order to achieve multicast function, you should enable IGMP Snooping, configure multicast VLAN, multicast router port, and so on. The requirement contains:  
multicast is VLAN 100.

Multicast server connects to uplink port 1.

ONU connects to PON 1.

Client, such as a PC, connects to ONU LAN 1.

### 2. Framework



### 3. Steps

(1) create VLAN

```
epon-olt(config)# vlan 100
epon-olt(config-vlan-100)# exit
```

(2) configure uplink port

```
epon-olt(config)# interface g 0/1
epon-olt(config-if-ge0/1)# switchport hybrid vlan 100 tagged
epon-olt(config-if-ge0/1)# exit
```

(3) configure PON port

```
epon-olt(config)# inter epon 0/1
epon-olt(config-pon-0/1)# switchport hybrid vlan 100 tagged
epon-olt(config-pon-0/1)# ip igmp snooping user-vlan 100 group-vlan 100 tagged
epon-olt(config-pon-0/1)# exit
```

(4) enable IGMP snooping

```
epon-olt(config)# ip igmp snooping enable
```

(5) configure multicast router port

```
epon-olt(config)# ip igmp snooping mrouter vlan 100 interface g 0/1
```

(6) configure ONU LAN port

```
epon-olt(config)# inter epon 0/1
epon-olt(config-pon-0/1)# onu 1 ctc eth 1 vlan mode tag
epon-olt(config-pon-0/1)# onu 1 ctc eth 1 vlan pvid 100 pri 0
epon-olt(config-pon-0/1)# onu 1 ctc eth 1 mc_vlan add 100
epon-olt(config-pon-0/1)# onu 1 ctc eth 1 mc_tagstrip enable
```

## 10. ACL Configuration

### 10.1 Overview

In order to filter data packages, network equipments need to setup a series of rules for identifying what need to be filtered. Only matched with the rules the data packages can be filtered. ACL can achieve this function. Matched conditions of ACL rules can be source address, destination address, Ethernet type, VLAN, protocol port, and so on.

These ACL rules also can be used in other situations, such as classification of stream in QoS. An ACL rule may contain one or several sub-rules, which have different matched conditions.

This device supports the following types of ACL.

- IP Standard ACL.
- IP Extended ACL.
- ACL based on MAC address
- ACL based on port binding.
- ACL based on QoS.

Limitation of each ACL rule:

ACL type	ACL index	Maxium rules
IP Standard ACL	0-999	1000
IP Extended ACL	1000-1999	1000
ACL based on MAC address	2000-2999	1000
ACL based on port binding	5000-5999	1000
ACL based on QoS	6000-6999	1000

### 10.2 ACL configuration

ACL configuration mainly includes:

- IP Standard ACL.
- IP Extended ACL.
- ACL based on MAC address
- ACL based on port binding.
- ACL based on QoS.
- ACL rule apply to port.

#### 10.2.1 IP standard ACL

Begin at privileged configuration mode, configure IP standard ACL as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.

Step 2	<b>access-list</b> <i>access-list-number</i>	Enter ACL configuration mode. <i>access-list-number</i> is ACL index.range:0-999.
Step 3	<b>subset ip</b> <b>(permit deny)&lt;A.B.C.D&gt;[net-mask]</b> <b>subset ip (permit deny) host</b> <b>&lt;A.B.C.D&gt;</b> <b>subset ip [permit deny] any</b>	Configure ACL rule. <A.B.C.D>: define based on source IP address and mask ACL rule. <b>Host</b> : define based on single IP address ACL rule. <b>Any</b> : define based on any source IP address ACL rule.
Step 4	<b>exit</b>	Exit to global configuration mode.
Step 5	<b>show access-list</b> [ <i>access-list-number</i>   <b>all</b> ]	Show ACL configurations.
Step 6	<b>write</b>	Save configurations.

### 10.2.2 IP extended ACL

Begin at privileged configuration mode, configure IP extended ACL as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>access-list</b> <i>access-list-number</i>	Enter ACL configuration mode. <i>access-list-number</i> is ACL index.range:1000-1999.
Step 3	<b>subset protocol {deny  permit}</b> <i>protocol</i> { <A.B.C.D> <i>net-mask</i> {<A.B.C.D> <i>net-mask</i> <b>host</b> <A.B.C.D>  <b>any</b> }[ <b>match</b> { <b>dscp priority</b>   <b>precedencepriority</b>   <b>tos</b> <i>priority</i> }] [ <b>set</b> { <b>dscp priority</b>   <b>precedence</b> <i>priority</i>   <b>tospriority</b> }]	Configure IP extended ACL rule. Parameter <i>protocol</i> should be icmp, igmp, igmp, ip, ospf, pim, tcp, or udp, etc. it also can be replaced by protocol code 0~255.
Step 4	<b>exit</b>	Exit global configuration mode.
Step 5	<b>show access-list</b> [ <i>access-list-number</i>   <b>all</b> ]	Show ACL configurations.
Step 6	<b>write</b>	Save configurations.

### 10.2.3 ACL based on MAC address

Begin at privileged configuration mode, configure ACL based on MAC address as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.

<b>Step 2</b>	<b>access-list</b> <i>access-list-number</i>	Enter ACL configuration mode. <i>access-list-number</i> is ACL index. range:2000-2999.
<b>Step 3</b>	<b>subset ethernet</b> [permit deny] [source] <xx:xx:xx:xx:xx:xx><xx:xx:xx:xx:xx:xx> {[dest] <xx:xx:xx:xx:xx:xx><xx:xx:xx:xx:xx:xx>}* 1 {[vlan] <1-4094>}*1 {[cos] <0-7>}*1 {[ethernet-type] <XXXX><XXXX>}	Configure IP extended ACL rule.
<b>Step 4</b>	<b>exit</b>	Exit to global configuration mode.
<b>Step 5</b>	<b>show access-list</b> [ <i>access-list-number</i>   <b>all</b> ]	Show ACL configurations.
<b>Step 6</b>	<b>write</b>	Save configurations.

### 10.2.4 ACL based on port binding

This type of ACL includes the other types.

Begin at privileged configuration mode, configure ACL based on port binding as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>access-list</b> <i>access-list-number</i>	Enter ACL configuration mode. <i>access-list-number</i> is ACL index. range:5000-5999;
<b>Step 3</b>	<b>subset port-business</b> [permit deny] {src-ip dest-ip   protocol   tos-dscp   src-mac   dest-mac   vlan   cos   ethernet-type   src-port   dest-port}	Permit:Permit data stream which match the rule passing through. Deny:Do not permit data stream which match the rule passing through. src-ip: source IP address dest-ip:destination IP address protocol:IP protocol type tos-dscp:IP priority src-mac:source MAC address dest-mac:destination MAC address vlan:VLAN IAD cos:802.1p priority ethernet-type:ethernet type src-port:Layer 4 source port dest-port:Layer 4 destination port
<b>Step 4</b>	<b>exit</b>	Exit to global configuration mode.
<b>Step 5</b>	<b>show access-list</b> <i>access-list-number</i>	Show ACL configurations.

<b>Step 6</b>	<b>write</b>	Save configurations.
---------------	--------------	----------------------

### 10.2.5 ACL based on QoS

Begin at privileged configuration mode, configure ACL based on QoS as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>access-list <i>access-list-number</i></b>	Enter ACL configuration mode. <i>access-list-number</i> is ACL index. range:6000-6999.
<b>Step 3a</b>	<b>subset qos &lt;0-8&gt;&lt;0-7&gt;&lt;1-12&gt;</b>	<0-8>: output priority <0-7>: output queue <1-12>: rule priority
<b>Step 3b</b>	<b>subset qos {src-ip dest-ip   protocol   tos-dscp   src-mac   dest-mac   vlan   cos   ethernet-type   src-port   dest-port}</b>	src-ip: source IP address dest-ip: destination IP address protocol: IP protocol type tos-dscp: IP priority src-mac: source MAC address dest-mac: destination MAC address vlan: VLAN ID cos:802.1p priority ethernet-type: Ethernet type src-port:Layer 4 source port dest-port:Layer 4 destination port
<b>Step 3c</b>	<b>no access-list <i>access-list-number</i></b>	Deleting ACL rule. Only the ACL that have not been applied can be deleted.
<b>Step 4</b>	<b>exit</b>	Exit to global configuration mode.
<b>Step 5</b>	<b>show access-list<i>access-list-number</i></b>	Show ACL configurations.
<b>Step 6</b>	<b>write</b>	Save configurations.

### 10.2.6 ACL rule apply to port

Begin at privileged configuration mode, apply ACL rule to port as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface {<i>interface_type slot/port</i>}</b>	Enter interface configuration mode.
<b>Step 3a</b>	<b>ip access-group<i>access-list-number</i> in</b>	Apply ACL rule to port.

<b>Step 3b</b>	<b>no ip access-group</b> <i>access-list-number</i> <b>in</b>	Delete ACL rule from port.
<b>Step 4</b>	<b>exit</b>	Exit to global configuration mode.
<b>Step 5</b>	<b>show access-list</b> <i>access-list-number</i>	Show ACL configurations.
<b>Step 6</b>	<b>write</b>	Save configurations.

### 10.3 Example

#### (1) Deny specific IP address packets passing through

PON1 denies packets which source IP is 192.168.100.10 passing through.

```
epon-olt(config)# access-list 5000
epon-olt(config-bsn-acl-5000)# subset port-business deny src-ip 192.168.100.10
255.255.255.255
epon-olt(config-bsn-acl-5000)# exit
epon-olt(config)# interface epon 0/1
epon-olt(config-pon-0/1)# ip access-group 5000 in
```

#### (2) Permit specific MAC address packets passing through

PON1 permits IP packets which source MAC is b8:97:5a:72:37:8d passing through.

```
epon-olt(config)# access-list 2000
epon-olt(config-eth-acl-2000)# subset ethernet deny ethernet-type 0800 ffff
epon-olt(config-eth-acl-2000)# exit
epon-olt(config)# access-list 2001
epon-olt(config-eth-acl-2001)# subset ethernet permit source b8:97:5a:72:37:8d
ff:ff:ff:ff:ff:ff
epon-olt(config-eth-acl-2001) # exit
epon-olt(config)# interface epon 0/1
epon-olt(config-pon-0/1)# ip access-group 2000 in
epon-olt(config-pon-0/1)# ip access-group 2001 in
epon-olt(config-pon-0/1)# exit
```

## 11. QoS Configuration

### 11.1 Configure queue scheduling mode

Queue scheduling mode contains strict priority, weighted round robin and hybrid mode. This device supports 8 queues altogether.

Begin at privileged configuration mode, configure queue scheduling mode as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2a</b>	<b>queue-scheduler strict-priority</b>	Configure strict priority scheduling mode.
<b>Step 2b</b>	<b>queue-scheduler wrr</b> [ <i>queue0 queue1 queue2 queue3 queue4 queue5 queue6 queue7</i> ]	Configure weighted round robin scheduling mode. <i>Queue<sub>x</sub></i> is weight of queue <i>x</i> , range is 1-127. By default, weights of queue 0~7 are 1, 1, 2, 2, 4, 4, 8, 8.
<b>Step 2c</b>	<b>queue-scheduler sp-wrr</b> [ <i>queue0 queue1 queue2 queue3 queue4 queue5 queue6 queue7</i> ]	Configure hybrid scheduling mode. <i>Queue<sub>x</sub></i> is weight of queue <i>x</i> , range is 0-127. If it is set to be 0, the queue is strict priority queue. By default, weights of queue 0~7 are 1, 1, 2, 2, 4, 4, 8, 8.
<b>Step 3</b>	<b>show queue-scheduler</b>	Show queue scheduling configurations.
<b>Step 4</b>	<b>write</b>	Save configurations.

### 11.2 Configure queue mapping

Begin at privileged configuration mode, configure queue mapping as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.

---

<b>Step 2</b>	<b>queue-scheduler tc <i>priority</i> queue <i>queue</i></b>	Configure mapping relation between queues and priority. By default, priority 0~7 maps to queue 0~7 respectively.
<b>Step 3</b>	<b>show queue-scheduler priority mapping</b>	Show queue mapping.
<b>Step 4</b>	<b>write</b>	Save configurations.

## 12.STP Configuration

### 12.1 STP default settings

STP default settings:

Speciality	Default value
Enable status	STP disabled
Bridge priority	32768
STP port priority	128
STP port cost	10-Gigabit Ethernet :2 Gigabit Ethernet :4 Fast Ethernet :19 Ethernet :100
Hello time	2s
Forward delay time	15s
Maxmum aging time	20s
Mode	RSTP

### 12.2 Cofigure STP

STP configurations mainly contain:

- Enable device's STP function.
- Enable port's STP function.
- Configure STP mode.
- Configure bridge priority of device.
- Configure forward delay of device.
- Configure hello time of device.
- Configure max age of designated device.
- Configure priority of designated port.
- Configure path cost of designated port.

#### 12.2.1 Enable device's STP function

Begin at privileged configuration mode, enable device's STP function as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2a	<b>spanning-tree on</b>	Enable device's STP function. By default, STP function is disabled.

Step 2b	<b>no spanning-tree</b>	Disable device's STP function.
Step 3	<b>show spanning-tree</b>	Show STP configurations.
Step 4	<b>write</b>	Save configurations.

### 12.2.2 Enable port STP

In order to work flexibly, you can disable some specific ports' STP function.

Begin at privileged configuration mode, enable port's STP function as the following table shows.

	<b>Command</b>	<b>Function</b>
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> { <i>interface_type slot/port</i> }	Enter interface configuration mode.
Step 3a	<b>spanning-tree on</b>	Enable port's STP function.
Step 3b	<b>no spanning-tree on</b>	Disable port's STP function.
Step 4	<b>exit</b>	Exit to global configuration mode.
Step 5	<b>show spanning-tree interface</b> { <i>interface_type slot/port</i> }	Show port's STP configurations.
Step 6	<b>write</b>	Save configurations.

### 12.2.3 Configure spanning tree mode

This device supports STP and RSTP. By default, it runs RSTP. You can choose RTP manually.

Begin at privileged configuration mode, configure spanning tree mode as the following table shows.

	<b>Command</b>	<b>Function</b>
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>spanning-tree mode</b> [rstp   stp]	Configure spanning tree mode. It runs RSTP by default.
Step 3	<b>show spanning-tree</b>	Show STP configurations.
Step 4	<b>write</b>	Save configurations.

### 12.2.4 Configure bridge priority

Device's bridge priority decides if it will be selected as root of spanning tree.

Begin at privileged configuration mode, configure device's bridge priority as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>spanning-tree priority</b> <i>bridge-priority</i>	Configure device's bridge priority. Priority range is 0~65535, default is 32768.
Step 3	<b>show spanning-tree</b>	Show STP configurations.
Step 4	<b>write</b>	Save configurations.

### 12.2.5 Configure forward delay

Network will recompute spanning tree when there is link down in network. Construction of spanning tree will be changed too. But the new STP PDU can't go the rounds of network. In this case, a temporary loop will come out if the new root port and designated port forward data immediately. So, STP adopts state transition mechanism. Before re-forwarding data, root port and designated port will undergo an intermediate state. After forward delay time out in the intermediate state, the new STP PDU have gone the rounds of network, then root port and designated port begin to forward data.

Begin at privileged configuration mode, configure device's forward delay as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>spanning-tree forward-time</b> <i>seconds</i>	Configure device's forward delay. bridge-priority range is 4~30, default is 15.
Step 3	<b>show spanning-tree</b>	Show STP configurations.
Step 4	<b>write</b>	Save configurations.

Forward Delay has something to do with that how big the network is. Generally, the bigger the network, the longer forward delay should be configured. If forward delay is too small, there may be temporary redundant path; while it is too big, network will take more time to resume connectivity. We suggest using default value if you have no idea about this.

#### Notice:

Hello time, forward delay and maximum age are time parameters of root device. These three parameters should meet the following formula, otherwise, the network will not stable.

$$2 \times (\text{forward-delay} - 1) \geq \text{maximum-age} \geq 2 \times (\text{hello} + 1)$$

The unit of "1" in formula is second.

### 12.2.6 Configure hello time

Network Bridge will send hello message to other surrounding network bridge at regular

intervals for verifying link connectivity. A suitable hello time can ensure a device find link failure in time and not occupy more network resource. If hello time is too big, device will be in mistake for link failure when loss packets. Then network device recomputes spanning tree. While if too small, network device sends repeated STP PDU frequently. This will increase device's load and waste network resource.

Begin at privileged configuration mode, configure device's hello time as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>spanning-tree hellotime <i>seconds</i></b>	Configure device's hello time. Hello time range is 1~10, default is 2.
<b>Step 3</b>	<b>show spanning-tree</b>	Show STP configurations.
<b>Step 4</b>	<b>write</b>	Save configurations.

### 12.2.7 Configure max age time

Max age time is maximum life time of configuration message. When message age is bigger than maximum age, configuration message will be discarded.

Begin at privileged configuration mode, configure maximum age as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>spanning-tree max-age <i>seconds</i></b>	Configure maximum age of device. max age range is 6-40, default is 20.
<b>Step 3</b>	<b>show spanning-tree</b>	Show STP configurations.
<b>Step 4</b>	<b>write</b>	Save configurations.

### 12.2.8 Configure priority of designated port

Port priority decides whether it can be selected as root port or not. On equal conditions, the higher priority port will be selected as root port. Generally, the priority value is smaller, the port has higher priority. If all ports' priority value are the same, their priority decided by their port index.

Begin at privileged configuration mode, configure priority of designated port as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.

<b>Step 2</b>	<b>interface</b> { <i>interface_type slot/port</i> }	Enter interface configuration mode.
<b>Step 3</b>	<b>spanning-tree port-priority</b> <i>priority</i>	Configure priority of designated port. priority range is 1-255, default is 128.
<b>Step 4</b>	<b>exit</b>	Exit to global configuration mode.
<b>Step 5</b>	<b>show spanning-tree interface</b> { <i>interface_type slot/port</i> }	Show port STP configurations.
<b>Step 6</b>	<b>write</b>	Save configurations.

### 12.2.9 Configure path cost of designated port

Path Cost is related to the speed of the link connected to the port. On the STP switch, a port can be configured with different path costs.

Begin at privileged configuration mode, configure path cost of designated port as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface</b> { <i>interface_type slot/port</i> }	Enter interface configuration mode.
<b>Step 3</b>	<b>spanning-tree cost</b> <i>value</i>	Configure path cost of designated port. Path cost range is 1-65535, default is auto.
<b>Step 4</b>	<b>exit</b>	Exit to global configuration mode.
<b>Step 5</b>	<b>show spanning-tree interface</b> { <i>interface_type slot/port</i> }	Show port STP configurations.
<b>Step 6</b>	<b>write</b>	Save configurations.

### 12.2.10 Configure edge port

The port which connects with terminal host is EdgePort. In process of spanning tree recomputation, edge port can transfer to forwarding status directly so that it can reduce transfer time. Because RSTP can't detect whether the port is edge port or not, if the port doesn't connect with switch, you'd better configure it as edge port. But when the port connects with a switch, RSTP can detect and configure it as non-edge port. By default, all ports are configured as non-edged port.

Begin at privileged configuration mode, configure edge port as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.

<b>Step 2</b>	<b>interface</b> { <i>interface_type slot/port</i> }	Enter interface configuration mode.
<b>Step 3a</b>	<b>spanning-tree operedge</b>	Configure port as an edge port.
<b>Step 3b</b>	<b>no spanning-tree operedge</b>	Reset spanning tree port to default.
<b>Step 4</b>	<b>exit</b>	Exit to global configuration mode.
<b>Step 5</b>	<b>show spanning-tree interface</b> { <i>interface_type slot/port</i> }	Show port STP configurations.
<b>Step 6</b>	<b>write</b>	Save configurations.

### 12.2.11 Configure point to point mode

Point to point mode is usually the link which connects with switches. For the ports connected with the point-to-point link, upon some port role conditions met, they can transit to forwarding state fast through transmitting synchronization packet, thereby reducing the unnecessary forwarding delay.

Begin at privileged configuration mode, configure port to connect with point to point link as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface</b> { <i>interface_type slot/port</i> }	Enter interface configuration mode.
<b>Step 3a</b>	<b>spanning-tree point-to-point</b>	Configure a port as point to point port. By default, all ports are configured as point to point ports.
<b>Step 3b</b>	<b>no spanning-tree point-to-point</b>	Not to configure a port as point to point port.
<b>Step 4</b>	<b>exit</b>	Exit to global configuration mode.
<b>Step 5</b>	<b>show spanning-tree interface</b> { <i>interface_type slot/port</i> }	Show port STP configurations.
<b>Step 6</b>	<b>write</b>	Save configurations.

### 12.3 Show STP information

After configuring, use the following commands to show STP information.

<b>Command</b>	<b>Function</b>
<b>show spanning-tree</b>	Show STP configurations and

---

	running status.
<b>show spanning-tree interface</b> <i>{interface_type slot/port}</i>	Show STP configurations and running status of a port.

## 13. OLT Management Configuration

### 13.1 Configure outband management

Port AUX is outband management port. So its IP is outband management IP.

#### 13.1.1 Enter AUX port configuration mode

Begin at privileged configuration mode, enter interface configuration mode as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface aux</b>	Enter AUX interface.

#### 13.1.2 Configure outband management IP address and mask

Begin at privileged configuration mode, configure outband management IP address and mask as the following table shows.

	Command	Function
Step 1	<b>config terminal</b>	Enter global configuration mode.
Step 2	<b>interface aux</b>	Enter AUX interface.
Step 3a	<b>ipaddress</b> <A.B.C.D> <i>net-mask</i>	Configure IP address and mask of AUX port.
Step 3b	<b>no aux ip address</b>	Reset outband management IP to default.
Step 4	<b>exit</b>	Exit to global configuration mode.
Step 5	<b>show aux ip address</b>	Show outband management IP.
Step 6	<b>write</b>	Save configurations.

#### 13.1.3 Configure Outband Management IPv6 Address

Begin at privileged configuration mode, configure outband management IPv6 address and mask as the following table shows.

	Command	Function
Step 1	<b>config terminal</b>	Enter global configuration mode.
Step 2	<b>interface aux</b>	Enter AUX port configuration

		mode.
Step 3a	<b>ipv6 address</b> <X:X::X:X> [eui-64]	Configure IPv6 address and prefix length of AUX port.
Step 3b	<b>no aux ipv6 address</b>	Delete IPv6 address of AUX port.
Step 4	<b>exit</b>	Exit to global configuration mode.
Step 5	<b>show aux ipv6 address</b>	Display AUX port configuration.
Step 6	<b>write</b>	Save configuration.

### 13.1.4 Show AUX port information

Begin at privileged configuration mode, show AUX port information as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>show interface aux</b>	Show AUX port information.

## 13.2 Configure inband management

This device provides inband management which can be managed from uplink port.

Begin at privileged configuration mode, configure inband management IP address and mask as the following table shows.

	Command	Function
Step 1	<b>config terminal</b>	Enter global configuration mode.
Step 2	<b>vlan</b> <i>vlan_id</i>	Create VLAN.
Step 3	<b>exit</b>	Exit to global configuration mode.
Step 4	<b>interface vlan</b> <i>vlan_id</i>	Enter VLAN interface configuration mode. <i>vlan_id</i> range is 1–4094.
Step 5a	<b>ipaddress</b> <A.B.C.D> <i>net-mask</i>	Configure IP address and mask.
Step 5b	<b>no ipaddress</b> <A.B.C.D>	Delete IP address and mask.
Step 6	<b>exit</b>	Exit to global configuration mode.
Step 7	<b>show interface vlan</b> <i>vlan_id</i>	Show VLAN information.
Step 8	<b>write</b>	Save configurations.

### 13.3 Configure management gateway

When OLT management IP and management server are not in the same network segment, it needs to configure a gateway.

Begin at privileged configuration mode, configure management gateway as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>config terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>gateway &lt;A.B.C.D&gt;</b>	Configure management gateway. <b>The gateway must be the same network segment with outband or inband management IP.</b>
<b>Step 3</b>	<b>no gateway</b>	Delete management gateway.
<b>Step 4</b>	<b>show gateway</b>	Show management gateway configuration.
<b>Step 5</b>	<b>write</b>	Save configurations.

## 14.L3 Route Configuration

### 14.1 Configuring L3 Interface

Begin at privileged configuration mode, configure L3 interface IP address and mask as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>config terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>vlan <i>vlan_id</i></b>	Create VLAN.
<b>Step 3</b>	<b>exit</b>	Exit to global configuration mode.
<b>Step 4</b>	<b>interface vlan <i>vlan_id</i></b>	Enter VLAN interface configuration mode. <i>vlan_id</i> range is 1 – 4094.
<b>Step 5a</b>	<b>ipaddress&lt;<i>A.B.C.D</i>&gt; <i>net-mask</i></b>	Configure IP address and mask.
<b>Step 5b</b>	<b>no ipaddress&lt;<i>A.B.C.D</i>&gt;</b>	Delete IP address and mask.
<b>Step 6</b>	<b>exit</b>	Exit to global configuration mode.
<b>Step 7</b>	<b>show interface vlan <i>vlan_id</i></b>	Show VLAN information.
<b>Step 8</b>	<b>write</b>	Save configurations.

### 14.2 ARP Proxy

Support the ONUs communication with each other under same PON port.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface vlan <i>vlan_id</i></b>	Enter VLAN interface configuration mode. <i>vlan_id</i> range is 1 – 4094.
<b>Step 3a</b>	<b>ip proxy-arp</b>	Enable arp proxy.
<b>Step 3b</b>	<b>no ip proxy-arp</b>	Disable arp proxy.
<b>Step 4</b>	<b>exit</b>	Exit to global configuration mode.

		mode.
<b>Step 5</b>	<b>write</b>	Save configurations.

### 14.3 Static Route

Static route is usually used in a simple network. This device supports maximum 512 static route rules.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2a</b>	<b>ip route</b> <i>A.B.C.D A.B.C.D A.B.C.D</i>	Add static route rule.
<b>Step 2b</b>	<b>ip route</b> <i>A.B.C.D/M A.B.C.D</i>	Add static route rule.
<b>Step 3a</b>	<b>no ip route</b> <i>A.B.C.D A.B.C.D A.B.C.D</i>	Delete static route rule.
<b>Step 3b</b>	<b>no ip route</b> <i>A.B.C.D/M A.B.C.D</i>	Delete static route rule.
<b>Step 4</b>	<b>show ip route</b>	Show route rules.

### 14.4 RIP Configuration

#### 14.4.1 Configuring Basic RIP Parameters

To configure RIP, you enable RIP routing for a network and optionally configure other parameters.

Beginning in privileged EXEC mode, follow these steps to enable and configure RIP:

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>router rip</b>	Enable a RIP routing process, and enter router configuration mode.
<b>Step 3</b>	<b>network</b> <i>ip-address/masklen</i>	Associate a network with a RIP routing process. You can specify multiple network commands. RIP routing updates are sent and received through interfaces only on these networks.
<b>Step 4</b>	<b>neighbor</b> <i>ip-address</i>	(Optional) Define a

		neighboring router with which to exchange routing information. This step allows routing updates from RIP (normally a broadcast protocol) to reach nonbroadcast networks.
<b>Step 5</b>	<b>offset-list</b> ( <i>access-list number</i>   <i>name</i> ) ( <b>in</b>   <b>out</b> ) <b>metric</b> <0-16> <b>vlan</b> <1-4094>	(Optional) Apply an offset list to routing metrics to increase incoming and outgoing metrics to routes learned through RIP. You can limit the offset list with an access list or an interface.
<b>Step 6</b>	<b>timers basic</b> <i>update timeout garbage</i>	(Optional) Adjust routing protocol timers. Valid ranges for all timers are 0 to 4294967295 seconds. <ul style="list-style-type: none"> <li>•<b>update</b>—Time between sending routing updates. The default is 30 seconds.</li> <li>•<b>invalid</b>—Time after which a route is declared invalid. The default is 180 seconds.</li> <li>•<b>holddown</b>—Time before a route is removed from the routing table. The default is 180 seconds.</li> <li>•<b>flush</b>—Amount of time for which routing updates are postponed. The default is 240 seconds.</li> </ul>
<b>Step 7</b>	<b>version</b> (1 2)	(Optional) Configure the switch to receive and send only RIP Version 1 or RIP version 2 packets. By default, the switch receives Version 1 and 2 but sends only Version 1. You can also use the interface commands <code>ip rip {send   receive} version 1   2   1 2</code> to control what versions are used for sending and receiving on

		interfaces.
<b>Step 8</b>	<b>redistribute</b> (kernel connected ospf static) {metric <0-16>}	(Optional) redistribute routes from kernel, connect, ospf and static.
<b>Step 9</b>	<b>distance</b> <1-255>	(Optional) Configure RIP protocol distance. Default 120.
<b>Step 10</b>	<b>exit</b>	Return to privileged EXEC mode.
<b>Step 11</b>	<b>show ip rip status</b>	Showing RIP current status. About the RIP timer, filter list, version, interface information.
<b>Step 12</b>	<b>show ip rip</b>	Showing RIP route information.
<b>Step 13</b>	<b>write</b>	Save configurations.

To turn off the RIP routing process, use the **no router rip** global configuration command.

#### 14.4.2 Configuring RIP Authentication

RIP version 1 does not support authentication. If you are sending and receiving RIP Version 2 packets, you can enable RIP authentication on an interface. The key chain determines the set of keys that can be used on the interface. If a key chain is not configured, no authentication is performed, not even the default.

The OLT supports two modes of authentication on interfaces for which RIP authentication is enabled: plain text and MD5. The default is plain text.

Beginning in privileged EXEC mode, follow these steps to configure RIP authentication on an interface:

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface</b> vlanvlan_id	Enter interface configuration mode, and specify the interface to configure.
<b>Step 3</b>	<b>ip rip authentication mode (md5  text )</b>	Configure the interface to use plain text authentication (the default) or MD5 digest authentication.
<b>Step 4a</b>	<b>ip rip authentication key-chain</b> < line>	Enable RIP authentication for MD5.
<b>Step 4b</b>	<b>ip rip authentication string</b> < line>	Enable RIP authentication for plain text.

Step 5	<b>exit</b>	Return to privileged EXEC mode.
Step 6	<b>show ip rip status</b>	Showing RIP current status. About the RIP timer, filter list, version, interface information.
Step 7	<b>show ip rip</b>	Showing RIP route information.
Step 8	<b>write</b>	Save configurations.

To restore clear text authentication, use the **no ip rip authentication mode** interface configuration command. To prevent authentication, use the **no ip rip authentication key-chain** interface configuration command.

### 14.4.3 Configuring Split Horizon

Routers connected to broadcast-type IP networks and using distance-vector routing protocols normally use the split-horizon mechanism to reduce the possibility of routing loops. Split horizon blocks information about routes from being advertised by a router on any interface from which that information originated. This feature usually optimizes communication among multiple routers, especially when links are broken.

Beginning in privileged EXEC mode, follow these steps to set an interface to configuring split horizon on the interface:

	<b>Command</b>	<b>Function</b>
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interfacevlan</b> <i>vlan_id</i>	Enter interface configuration mode, and specify the interface to configure.
Step 3	<b>ip rip split-horizon</b>	Enable split horizon. Default enable.
Step 5	<b>exit</b>	Return to privileged EXEC mode.
Step 6	<b>show ip rip status</b>	Showing RIP current status. About the RIP timer, filter list, version, interface information.
Step 7	<b>show ip rip</b>	Showing RIP route information.
Step 8	<b>write</b>	Save configurations.

To disable split horizon, use the **no ip rip split-horizon** interface configuration command.

#### 14.4.4 Configuring RIP v1/2 Compatible

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface vlan <i>vlan_id</i></b>	Enter interface configuration mode, and specify the interface to configure.
<b>Step 3</b>	<b>ip rip receive version (1 2) (1 2)</b>	Configure receive v1 or v2 or v1 and v2.
<b>Step 4</b>	<b>ip rip send version (1 2) (1 2)</b>	Configure send v1 or v2 or v1 and v2.
<b>Step 5</b>	<b>exit</b>	Return to privileged EXEC mode.
<b>Step 6</b>	<b>show ip rip status</b>	Showing RIP current status. About the RIP timer, filter list, version, interface information.
<b>Step 7</b>	<b>show ip rip</b>	Showing RIP route information.
<b>Step 8</b>	<b>write</b>	Save configurations.

## 14.5 OSPF Configuration

### 14.5.1 Configuring Basic OSPF Parameters

Enabling OSPF requires that you create an OSPF routing process, specify the range of IP addresses to be associated with the routing process, and assign area IDs to be associated with that range.

Beginning in privileged EXEC mode, follow these steps to enable OSPF:

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>router ospf</b>	Enable OSPF routing, and enter router configuration mode.
Step 3	<b>router-id</b> <i>A.B.C.D</i>	(Optional)Configure router id.
Step 4	<b>network</b> <i>A.B.C.D/Marea(A.B.C.D &lt;0-4294967295&gt;)</i>	Define an interface on which OSPF runs and the area ID for that interface. The area ID can be a decimal value or an IP address.
Step 5	<b>exit</b>	Return to privileged EXEC mode.
Step 6	<b>write</b>	Save configurations.

To terminate an OSPF routing process, use the **no router ospf** global configuration command.

### 14.5.2 Configuring OSPF Interfaces

You can use the ip ospf interface configuration commands to modify interface-specific OSPF parameters. You are not required to modify any of these parameters, but some interface parameters (hello interval, dead interval, and authentication key) must be consistent across all routers in an attached network. If you modify these parameters, be sure all routers in the network have compatible values.

Beginning in privileged EXEC mode, follow these steps to modify OSPF interface parameters:

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface vlan</b> <i>vlan_id</i>	Enter interface configuration mode, and specify the Layer 3

		interface to configure.
<b>Step 3</b>	<b>ip ospf cost</b> <1-65535>	(Optional) Explicitly specify the cost of sending a packet on the interface.
<b>Step 4</b>	<b>ip ospf retransmit-interval</b> <i>seconds</i>	(Optional) Specify the number of seconds between link state advertisement transmissions. The range is 1 to 65535 seconds. The default is 5 seconds.
<b>Step 5</b>	<b>ip ospf transmit-delay</b> <i>seconds</i>	(Optional) Set the estimated number of seconds to wait before sending a link state update packet. The range is 1 to 65535 seconds. The default is 1 second.
<b>Step 6</b>	<b>ip ospf priority</b> <i>number</i>	(Optional) Set priority to help determine the OSPF designated router for a network. The range is from 0 to 255. The default is 1.
<b>Step 7</b>	<b>ip ospf hello-interval</b> <i>seconds</i>	(Optional) Set the number of seconds between hello packets sent on an OSPF interface. The value must be the same for all nodes on a network. The range is 1 to 65535 seconds. The default is 10 seconds.
<b>Step 8</b>	<b>ip ospf dead-interval</b> <i>seconds</i>	(Optional) Set the number of seconds after the last device hello packet was seen before its neighbors declare the OSPF router to be down. The value must be the same for all nodes on a network. The range is 1 to 65535 seconds. The default is 4 times the hello interval.
<b>Step 9</b>	<b>ip ospf authentication-key</b> <i>auth_key</i>	(Optional) Assign a password to be used by neighboring OSPF routers. The password can be any string of keyboard-entered characters up to 8 bytes in length. All

		neighboring routers on the same network must have the same password to exchange OSPF information.
Step 10	<b>ip ospf message-digest-key</b> <i>keyid md5key</i>	(Optional) Enable MDS authentication. • <i>keyid</i> —An identifier from 1 to 255. • <i>key</i> —An alphanumeric password of up to 16 bytes.
Step 11	<b>ip ospf authentication</b>	Enable ospf authentication.
Step 12	<b>ip ospf authentication message-digest</b>	Enable ospf MD5 authentication.
Step 13	<b>exit</b>	Return to privileged EXEC mode.
Step 14	<b>show ip ospf interface</b> <i>[interface-name]</i>	Display OSPF-related interface information.
Step 15	<b>write</b>	Save configurations.

### 14.5.3 Configuring OSPF Area Parameters

You can optionally configure several OSPF area parameters. These parameters include authentication for password-based protection against unauthorized access to an area, stub areas, and not-so-stubby-areas (NSSAs). Stub areas are areas into which information on external routes is not sent. Instead, the area border router (ABR) generates a default external route into the stub area for destinations outside the autonomous system (AS). An NSSA does not flood all LSAs from the core into the area, but can import AS external routes within the area by redistribution.

Route summarization is the consolidation of advertised addresses into a single summary route to be advertised by other areas. If network numbers are contiguous, you can use the area range router configuration command to configure the ABR to advertise a summary route that covers all networks in the range.

Beginning in privileged EXEC mode, follow these steps to configure area parameters:

	<b>Command</b>	<b>Function</b>
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>router ospf</b>	Enable OSPF routing, and enter router configuration mode.
Step 3	<b>area</b> <i>area-id</i> <b>authentication</b>	(Optional) Allow

		password-based protection against unauthorized access to the identified area. The identifier can be either a decimal value or an IP address.
<b>Step 4</b>	<b>area</b> <i>area-id</i> <b>authentication message-digest</b>	(Optional) Enable MD5 authentication on the area.
<b>Step 5</b>	<b>area</b> <i>area-id</i> <b>stub</b> [ <i>no-summary</i> ]	(Optional) Define an area as a stub area. The <i>no-summary</i> keyword prevents an ABR from sending summary link advertisements into the stub area.
<b>Step 6</b>	<b>area</b> <i>area-id</i> <b>nssa</b> [ <i>no-summary</i> ]	(Optional) Defines an area as a not-so-stubby-area. Every router within the same area must agree that the area is NSSA. Select one of these keywords: <ul style="list-style-type: none"> <li>• <i>no-summary</i>—Select to not send summary LSAs into the NSSA.</li> </ul>
<b>Step 7</b>	<b>area</b> <i>area-id</i> <b>range</b> <i>address/mask</i> <i>len</i>	(Optional) Specify an address range for which a single route is advertised. Use this command only with area border routers.
<b>Step 8</b>	<b>exit</b>	Return to privileged EXEC mode.
<b>Step 9</b>	<b>show running ip ospf</b>	Display OSPF running-config information.
<b>Step 10</b>	<b>show ip ospf database</b>	Display lists of information related to the OSPF database for a specific router.
<b>Step 11</b>	<b>write</b>	Save configurations.

Use the **no** form of these commands to remove the configured parameter value or to return to the default value.

### 14.5.4 Configuring OSPF Other Parameters

You can optionally configure other OSPF parameters in router configuration mode.

- Virtual links: In OSPF, all areas must be connected to a backbone area. You can establish a virtual link in case of a backbone-continuity break by configuring two Area Border Routers as endpoints of a virtual link. Configuration information includes the identity of the other virtual endpoint (the other ABR) and the nonbackbone link that the two routers have in common (the transit area). Virtual links cannot be configured through a stub area.
- Default route: When you specifically configure redistribution of routes into an OSPF routing domain, the route automatically becomes an autonomous system boundary router (ASBR). You can force the ASBR to generate a default route into the OSPF routing domain.
- Administrative distance is a rating of the trustworthiness of a routing information source, an integer between 0 and 255, with a higher value meaning a lower trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. OSPF uses three different administrative distances: routes within an area (interarea), routes to another area (interarea), and routes from another routing domain learned through redistribution (external). You can change any of the distance values.

Beginning in privileged EXEC mode, follow these steps to configure these OSPF parameters:

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>router ospf</b>	Enable OSPF routing, and enter router configuration mode.
Step 3	<b>area</b> <i>area-id</i> <b>virtual-link</b> <i>A.B.C.D</i>	(Optional) Establish a virtual link and set its parameters.
Step 4	<b>default-information originate</b> {[ <b>always</b> ]}*1 {[ <b>metric</b> <0-16777214>]*1} {[ <b>metric-type</b> (1 2)]*1} {[ <b>route-map</b> <WORD>]*1}	(Optional) Force the ASBR to generate a default route into the OSPF routing domain. Parameters are all optional.
Step 5	<b>distance ospf</b> {[ <b>inter-area</b> <i>dist1</i> ] [ <b>inter-area</b> <i>dist2</i> ] [ <b>external</b> <i>dist3</i> ]}	(Optional) Change the OSPF distance values. The default distance for each type of route is 110. The range is 1 to 255.
Step 8	<b>exit</b>	Return to privileged EXEC mode.
Step 9	<b>show running ip ospf</b>	Display OSPF running-config information.
Step 10	<b>show ip ospf database</b>	Display lists of information related to the OSPF database for a specific router.

<b>Step 11</b>	<b>write</b>	Save configurations.
----------------	--------------	----------------------

### 14.5.5 Monitoring OSPF

You can display specific statistics such as the contents of IP routing tables, databases.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>show ip ospf database [router] [self-originate]</b> <b>show ip ospf database [router] [adv-router [ip-address]]</b> <b>show ip ospf database [network] [self-originate]</b> <b>show ip ospf database [network] [adv-router [ip-address]]</b> <b>show ip ospf database [summary] [self-originate]</b> <b>show ip ospf database [summary] [adv-router [ip-address]]</b> <b>show ip ospf database [asbr-summary] [self-originate]</b> <b>show ip ospf database [asbr-summary] [adv-router [ip-address]]</b> <b>show ip ospf database [external] [self-originate]</b> <b>show ip ospf database [external] [adv-router [ip-address]]</b>	Display lists of information related to the OSPF database.
<b>Step 3</b>	<b>show ip ospf route</b>	Display lists of information related to the OSPF route.
<b>Step 4</b>	<b>show ip ospf interface [interface-name]</b>	Display OSPF-related interface information.
<b>Step 5</b>	<b>show ip ospf neighbor</b>	Display OSPF interface neighbor information.

## 14.6 Manipulate routing selection updates

This section describes the direct routing redistribution of different routing protocols. Methods of controlling routing information sent between different routing selection protocols include using distribution lists, using routing mapping tables, and modifying administrative distances.

### 14.6.1 Routing IP List

#### 14.6.1.1 Access Control List Configuration

Access lists are typically used to control user data flows, but access lists do not affect the data flows generated by the current router. At the end is an implicit deny any statement. The access-list List has two standards and extensions:

- 1) value range of standard index: 1-99, 1300-1999, controlling only the source IP;
- 2) value range of extended index: 100-199, 2000-2699, control source IP and destination IP;

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2a	<b>ip access-list</b> <i>access_list_index</i> <b>{permit deny}</b> <A.B.C.D> <wildcard_mask>  <b>ip access-list</b> <i>access_list_index</i> <b>{permit deny}</b> <b>host</b> <A.B.C.D>  <b>ip access-list</b> <i>access_list_index</i> <b>{permit deny}</b> <b>any</b>	Define a standard access-list, <i>access_list_index</i> ranges from 1-99 to 1300-1999, < A.B.C.D. > < wildcard_mask > defines standard IP access based on the source IP address or mask; Host defines standard IP access based on a single source IP address; Any standard IP access based on any source IP address;
Step 2b	<b>ip access-list</b> <i>access_list_index</i> <b>{permit deny}</b> <A.B.C.D> <wildcard_mask> {<A.B.C.D> < <i>wildcard_mask</i> >   <b>host</b> <A.B.C.D>   <b>any</b> }  <b>ip access-list</b> <i>access_list_index</i> <b>{permit deny}</b> <b>host</b> <A.B.C.D> {<A.B.C.D> <wildcard_mask>   <b>host</b> <A.B.C.D>   <b>any</b> }  <b>ip access-list</b> <i>access_list_index</i> <b>{permit deny}</b> <b>any</b> {<A.B.C.D> <wildcard_mask>   <b>host</b> <A.B.C.D>   <b>any</b> }	Define an extended access-list, <i>access_list_index</i> ranges from 100-199 to 2000-2699, < A.B.C.D. > < wildcard_mask > defines extended IP access based on the source IP address or mask; Host defines extended IP access based on a single source IP address; Any extended IP access based on any source IP address;

	<b>no ip access-list</b> <i>access_list_index</i>	Delete access-list
<b>Step 3</b>	<b>exit</b>	Return to privileged EXEC mode.
<b>Step 4</b>	<b>show ip access-list</b>	Show access-list information
<b>Step 5</b>	<b>write</b>	Save configurations.

### 14.6.1.2 Prefix List Configuration

Prefix lists are similar to access lists, and the benefits of prefix lists include improved performance when loading and finding large lists, incremental update support, and greater flexibility. Filtering through the prefix list requires matching the routing prefix to the prefix listed in the prefix list, just as matching the access list. When there is a match, use routing.

By default, serial Numbers are generated automatically and incremented by 5. If automatic sequence number generation is disabled, you must specify a sequence number for each entry. You do not need to specify a serial number when deleting a configuration item.

The Prefix-List is identified by the Prefix List name, which can contain multiple table items. Each table item, in the form of a network prefix, specifies a matching range independently and is identified by a sequence\_num. Sequence\_num indicates the order in which matching checks are performed in the Prefix-List. Each table item has a "or" relationship, and during the match, the route checks sequence\_num in ascending order for each table item identified by sequence\_num. As long as one of the table items satisfies the condition, this means that the Prefix-List filter (which does not enter the match of the next table item) is passed.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2a</b>	<b>ip prefix-list</b> <i>prefix_list_name</i> [ <b>seq</b> <i>sequence_num</i> ] { <b>permit</b>   <b>deny</b> } < <i>A.B.C.D/M</i> > <b>[ge</b> <i>ge_value</i> <b>]</b> [ <b>le</b> <i>le_value</i> <b>]</b>  <b>ip prefix-list</b> <i>prefix_list_name</i> [ <b>seq</b> <i>sequence_num</i> ] { <b>permit</b>   <b>deny</b> } <b>any</b>	Create a list of prefixes with optional serial Numbers to deny or allow access to matching conditions.  The sequence_num range is 1-4294967295; The ge_value range is 0-32; The range of le_value is 0-32; Ge and le values specify the range of prefix lengths to match, and the specified ge values and values must satisfy: Prefix_len < ge_value < le_value < 32.

<b>Step 2b</b>	<b>no ip prefix-list</b> <i>prefix_list_name</i>	Delete prefix-list
<b>Step 3</b>	<b>exit</b>	Return to privileged EXEC mode.
<b>Step 4</b>	<b>show ip prefix-list</b> [ <b>detail</b>   <b>summary</b> ]	Show ip prefix-list information.
<b>Step 5</b>	<b>write</b>	Save configurations.

To remove the prefix list and all its entries, use the `no IP prefix-list prefix_list_name` command.

The keywords `ge` and `le` are optional and are used to specify the range of prefix lengths to match, which must satisfy the condition: `length < ge-value < le-value <=32`.

1. IP prefix-list 2 permit 2.2.2.2.0/24 //(match the first 24 bits: 2.2.\*, mask must be 24 bits)
2. IP prefix-list 2 permit 2.2.2.2.2/24 ge 25 le 30 //(match the first 24 bits :2.2.2.\*, mask must be 25-30 bits)
3. IP prefix-list 2 permit 2.2.2.2/24 le 32 //(match the first 24 bits :2.2.2.\*, mask must be 24-32 bits)
4. IP prefix-list 2 permit 2.2.2.2.2/24 ge 26 //(match the first 24 bits :2.2.2.\*, mask must be 26-32 bits)
5. IP prefix-list 3 permit 0.0.0.0.0/0 le 32 //(matches all)

## 14.6.2 Route Redistribution

Redistribution refers to the ability of boundary routers connected to different routing selection domains to exchange and notify routing selection information between different routing selection domains (autonomous systems). Redistribution is always outward, and the router performing the redistribution does not modify its routing selection table. Router configuration command: **default-metric\_** is used to specify the seed metric values for all redistribution routes. Specify the seed metric values in a **redistribute**, for which you can use the option `metric` or routing mapping table.

**Manage distance.** When using routing redistribution, it may occasionally be necessary to modify the protocol's administrative distance to make it a priority.

**Seed measurements.** When routing redistribution occurs, metrics must be specified for the rerouting route. This measure, called the seed measure or default measure, is defined during the redistribution configuration. After specifying the seed measure for the redistribute route, the measure will increase normally within the autonomous

system. The only exception is the OSPF E2 routing, which keeps the initial value regardless of how far it is propagated within the autonomous system.

**Default seed measurements.** RIP, IGRP, and EIGRP default to treat the seed metric value 0 as infinity. An infinite number of measurements indicate to the router that the reroute is unreachable and therefore should not be notified. Therefore, when rerouting the route to RIP, IGRP, and EIGRP, it is necessary to manually specify its seed measurement value, otherwise the rerouting route will not be notified. In OSPF, the redistributed routing defaults to 2 classes (E2), with a measurement value of 20. Except for the redistributed BGP routing, which defaults to 2 classes and measures 1.

**Redistribute technology.** Bidirectional redistribute: redistribute all routes between two routing selection processes. One-way redistribution: a default route is passed to a routing selection protocol, and only the network that is known through the routing protocol is passed to the other routing selection protocols.

**Passive interface:** on OSPF routers, allocation of passive - interface is used to make a specific interface can't accept that sends hello packets, also cannot form a neighbor relationship, using scene: 1: make a specific router interface does not participate in the process of routing protocol 2: without any neighbor relationship was established through a particular interface at the same time, also can notice of these interfaces are routing.

#### 14.6.2.1 RIP Route Redistribution

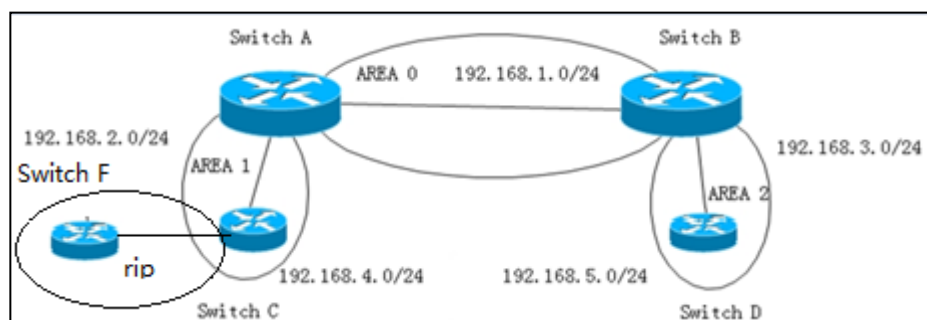
	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>router rip</b>	Start RIP and enter RIP configuration mode
Step 3	<b>distance</b> <1-255>	Set the administrative distance, default is 120.
Step 4	<b>default-metric</b> <1-16>	Default measurement
Step 5	<b>redistribute</b> ( <i>kernel connected static ospf</i> ) <b>{metric</b> <0-16>*1 <b>{route-map</b> <map-tag>*1	Inter-protocol routing redistribution, including direct connection, kernel, ospf protocol, static routing information to rip protocol. Let rip be published.
Step 6	<b>passive-interface</b> <IFNAME> {A.B.C.D}*1	Configure the passive interface

Step 7	<b>offset-list</b> (<access-list>) (in out) <0-16> {vlan <1-4094>}*1	Used to adjust measurements
Step 8	<b>show running-config</b>	Show running-config information

#### 14.6.2.2 OSPF Route Redistribution

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>router ospf</b>	Start ospf and enter ospf configuration mode
Step 3	<b>distance</b> <1-255>	Set the administrative distance, default is 110.
Step 4	<b>default-metric</b> <0-16777214>	Used to specify the seed metric values for all redistribution routes
Step 5	<b>redistribute</b> (kernel connected ospf static) {metric <0-16>} { <b>route-map</b> <map-tag>}*1	Inter-protocol routing redistribution, including redistribution of direct connection, kernel, ospf protocol, static routing information to rip protocol. Get the ospf protocol out there.
Step 6	<b>passive-interface</b> <IFNAME> {A.B.C.D}*1	Configure the passive interface
Step 7	<b>show running-config</b>	Show running-config information

For example:



Configuration	Result
switch c: router ospf router-id 3.3.3.3 network 192.168.2.3/24 area 1	When configured with metric of 30 on switch c, On switch a: O E2 192.168.4.0/24 [110/30] via 192.168.2.3, 01:01:27, Vlan2

redistribute connected metric 30(10) redistribute rip metric 30(10)	When configured with metric of 10 on switch c, On switch a: O E2 192.168.4.0/24 [110/10] via 192.168.2.3, 01:01:27, Vlan2
--	--

### 14.6.3 Use The Distribution List To Control Routing Selection Updates

A distribute-list distribution list is a tool used to control routing updates, filtering only routing information, not LSA. Therefore, it is suitable for distance vector routing protocols, such as RIP and EIGRP. Like the OSPF link state routing protocol, the IN direction (which affects local routing tables but is present IN LSDB), the OUT direction does not work. But local originating routes can be filtered because of reroute routing, not LSA delivery. The **distribute-list out** command filters routing selection updates from outbound routing updates from the interface or specifies routing selection updates for routing selection protocols; The **distribute-list in** command filters routing selection updates coming in from the specified interface.

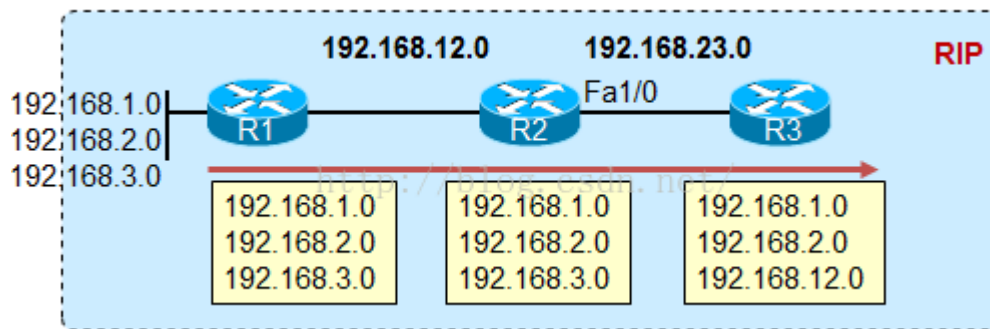
#### 14.6.3.1 Distance Vector Routing Protocol RIP

Routing information is passed between routers, and the distribution list has absolute control over routing information. So if it is in the direction, then through the deployment of distribution list, can filter the particular route, the executive distribution lists local routing routing table changes, at the same time, the local router in a routing update message to downstream routers, actually updated content is affected by the distribution list after entry. And in the out direction, there's no problem.

RIP's distribution list command:

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode..
Step 2	<b>router rip</b>	Start RIP and enter RIP configuration mode
Step 3	<b>distribute-list &lt;access-list&gt; (in out) {&lt;ifname&gt;}*1</b>	Filter routing using the access control list
Step 4	<b>distribute-list prefix &lt;prefix-list&gt; (in out) {&lt;WORD&gt;}*1</b>	Filter routing using prefix lists
Step 5	<b>show running-config</b>	Show running-config information

Configuration example 1 (in a single routing protocol environment-RIP)

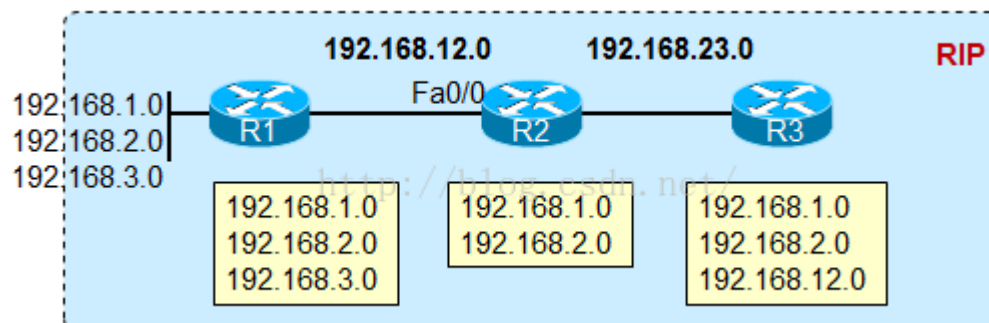


Initially, R3 was able to learn the three loopback routes of R1, as well as the 192.168.12.0/24 routes. Now we don't want R3 to learn 192.168.3.0/24 routing, so we can configure R2 as follows:

```
R2(config)# access-list 1 deny 192.168.3.0
R2(config)# access-list 1 permit any
R2 (config) # router rip
R2(config-router)# redistribute -list 1 out ethv0.3
```

Of course, in - oriented distribution lists can have the same effect in R3.

**Configuration example 2 (in a single routing protocol environment-RIP)**



In R2, if the following configuration is made:

```
R2(config)# access-list 1 deny 192.168.3.0
R2(config)# access-list 1 permit any
R2 (config) # router rip
R2(config-router)# redistribute -list 1 in ethv0.3
```

So, first of all, R2's own routing table will change, and 3.0's routing will be filtered out, and R3, the downstream RIP router, won't learn 3.0.

### 14.6.3.2 Link Status Routing Protocol OSPF

It is important to note that for such link-state routing protocol OSPF, routers communicate news is no longer routing information, but the LSA, and the distribution list cannot be to filter the LSA. Therefore, to deploy the distribution list in the link status protocol, you need to pay attention to:

**In direction**, distribution list only after receiving the LSA, locally generated route routed the moment of filtering, perform distribution list router routing table will be affected by the distribution list (local LSDB still is LSA), and the router will send the LSA LSADB to neighbors, so local routing are filtered, and neighbors.

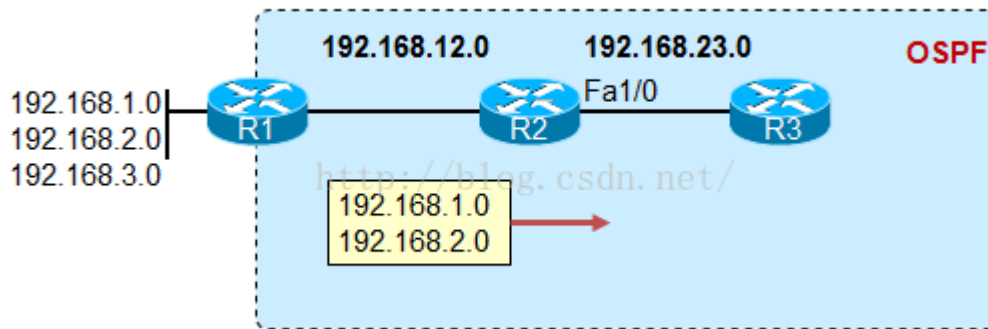
**Out direction**, the distribution list can only work on the ASBR that performs the routing reissue action, and only works for externally introduced routes. Because when performing redistribute, OSPF actually these exterior routing is introduced in the form of routing in, so the distribution list can work normally in this situation, but if not local originating exterior routing, or internal OSPF routing, out the direction of the distribution list are baffled.

For example, redistributing direct links to OSPF on R1 can filter out the external route of 1.1.1.0 with the out distribution list. However, if R1 republishes the incoming route, it cannot block R3 acceptance routing or LSA with an out distribution list on R2, because this is not an external route originating locally.

OSPF distribution list command:

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode..
<b>Step 2</b>	<b>router ospf</b>	Start ospf and enter ospf configuration mode
<b>Step 3</b>	<b>distribute-list &lt;access-list&gt; out (kernel connected static rip)</b>	Use the access control list for redistribution
<b>Step 5</b>	<b>show running-config</b>	Show running-config information

**Configuration example 1** --OSPF out directional distribution list in a single routing protocol environment



Distribution list, deployed in a link state routing protocol such as OSPF, can only be used if the out direction is used.

Pictured above, deployed on R1, R1 use redistribute direct way to introduce these three exterior routing and then out the direction of the distribution list, will be deployed on R1, and have effect on the three routing.

```
R1(config)# access-list 1 deny 192.168.3.0
```

```
R1(config)# access-list 1 permit any
```

```
R1 # router ospf (config)
```

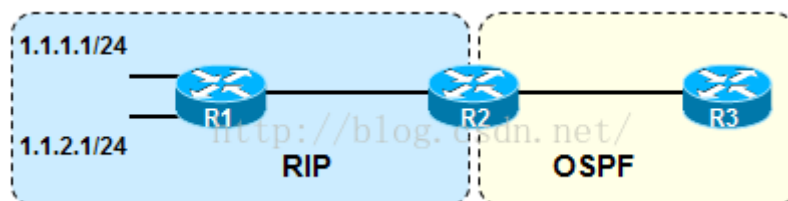
```
R1 (config - the router) # redistribute connected subnets
```

```
R1(config-router)# network 192.168.12.1 255.255.255.0 area 0
```

```
R1 (config - the router) # distribute - list out 1
```

After the above configuration is implemented, R1 will filter out the 3.0 routing.

**Configure example 2** -- deploy the distribution list when republished between protocols



RIP redistributes into OSPF

Case 1

R2 is configured as follows:

```
Access - the list 1 permit 1.1.1.0
```

```
The router ospf
```

```
Redistribute rip metric 10 subnets
```

```
Distribute - list 1 out rip
```

What this command means here is that only 1.1.1.0 is allowed out of the reroute from the RIP routing protocol (to the OSPF protocol, there is no direction, as long as the interface running the OSPF)

In R3, there are only 1.1.1.0 routes

Case 2

Open loopback interface 2.2.2.2/24 on R2, R2 reissues RIP into OSPF and reissues direct access to OSPF

Access - the list 1 permit 1.1.1.0

The router ospf

Redistribute connected subnets

Redistribute rip metric 10 subnets

Network 192.168.23.0 0.0.255 area 0

Distribute - list out 1

// there are only 1.1.1.0 routes in R3, that is, the command redistribute -list 1 out here works for all routes injected from outside into the OSPF, and only 1.1.0 routes survive. The source of continuous routing is direct connection routing, or RIP.

Case 3

Open loopback interface 2.2.2.2/24 on R2, R2 reissues RIP into OSPF and reissues direct access to OSPF

Access - the list 1 permit 1.1.1.0

The router ospf

Redistribute connected subnets

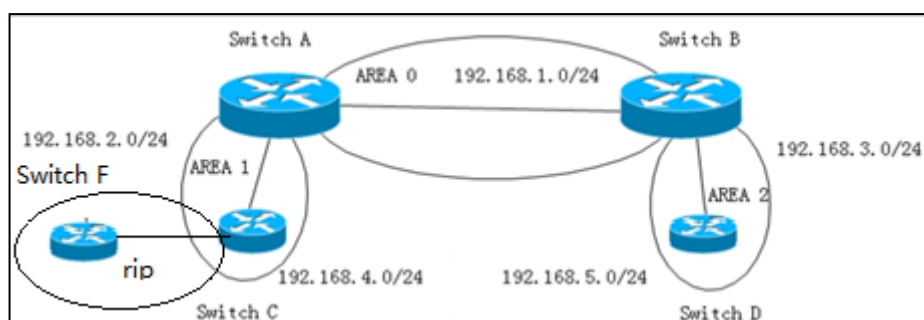
Redistribute rip metric 10 subnets

Distribute - list 1 out rip

// R3 has routing in the routing table: 1.1.1.0, 2.2.0, 192.168.12.0

// that is, the routing other than 1.1.1.0 that was re-published from RIP was blocked and the local direct connection port was republished

### Configuration example 3:



Configuration	Result
---------------	--------

<pre>Configure switch c: ip access-list 1 deny 192.168.6.0 0.0.0.255 ip access-list 1 permit any router ospf   ospf router-id 3.3.3.3   redistribute connected metric 30   redistribute rip metric 30   network 192.168.2.3/24 area 0.0.0.1   distribute-list 1 out rip</pre>	<pre>Result: Switch b: Unable to learn 192.168.6.0 segment of switch f; Learned 192.168.7.0 segment of switch f;</pre>
---	--

## 14.6.4 Use Routing Mapping Tables To Control Routing Selection Updates

### 14.6.4.1 Routing Map Configuration

Route Map can be used for rerouting and policy routing of routing, and is often used in BGP. Routing is actually complex static routing strategy, static routing is based on the packet destination address and forwarded to the designated the next-hop route, policy routing can provide various types of filtering and classification.

Switch can run multiple routing protocols simultaneously, redistributing information from one routing protocol to another. For example, you can reread igrp-derived routing by using RIP or by re-reading the static path instruction transformation using IGRP. Redistribution of information from one routing protocol to another applies to all supported ip-based routing protocols.

By defining routing mappings between two domains, you can conditionally control routing redistribution between routing domains. Match and set the condition part of the Route Map configuration command that defines the roadmap. The Match command specifies that a standard must be matched; The Set command specifies the action to be taken if the routing update satisfies the conditions defined by the matching command. Although redistribution is a protocol independent feature, some matching and setting of the Route Map configuration commands are protocol specific.

One or more matching commands and one or more Set commands follow a Route Map command. If there is no matching command, all of them match. If no command is set, nothing is done except for a match. Therefore, you need at least one match or setup command.

Like the access list, there is an implicit deny any statement at the end of the routing mapping table, which results in a result that depends on the purpose of the routing mapping table.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>route-map <i>map_name</i> [permit deny] <i>sequence_number</i></b>	Configure a route-map and enter the route-map configuration mode.

Step 3	<b>match ip address</b> <i>access_list_number</i>	Matching the specified access-list, the range of <i>access_list_number</i> is 1-2699, where 1-99 and 1300-1999 are standard access-list, and 100-199 and 2000-2699 are extended access-list.
Step 4	<b>match ip address prefix-list</b> <i>prefix_list_name</i>	Match the specified prefix-list.
Step 5	<b>match ip next-hop</b> <i>access_list_number</i>	Matching the next hop routing address through the specified access-list, the <i>access_list_number</i> range is 1-2699, where 1-99 and 1300-1999 are standard access-list, 100-199 and 2000-2699 are extended access-list.
Step 6	<b>match ip next-hop prefix-list</b> <i>prefix_list_name</i>	Match the next hop routing address through the specified prefix-list.
Step 7	<b>match interface</b> <i>interface_name</i>	Matches the routing of the next outgoing interface that is one of the specified interfaces
Step 8	<b>match metric</b> <i>metric_value</i>	Matching the specified routing metrics, <i>metric_value</i> ranges from 0-4294967295.
Step 9	<b>match tag</b> <i>tag_value</i>	Matches the specified routing tag, and the <i>tag_value</i> range is 1-4294967295.
Step 10	<b>set metric</b> <i>metric_value</i>	Set the metrics for the reroute routing, and <i>metric_value</i> ranges from 0-4294967295.
Step 11	<b>set metric-type</b> <i>metric_type</i>	Sets the measurement value type for the redistributed routing.
Step 12	<b>set tag</b> <i>tag_value</i>	Sets the tag for the redistributed routing.
Step 13	<b>set ip next-hop</b> <i>metric_value</i>	Specifies the measure of the next hop of forwarding.
Step 14	<b>exit</b>	Return to privileged EXEC



!		via
route-map test1 permit 30	192.168.1.1, ethv0.1	
match ip address 2	2)switch c execute: redistribute rip route-map	
set metric 500	test2	
!	switch b result	
route-map test2 permit 20	N E2 192.168.7.0/24	[2/500] tag: 0
match ip address 2		via
set metric 500	192.168.1.1, ethv0.1	
!	3)switch c execute: redistribute rip route-map	
route-map test3 permit 40	test3	
match ip address prefix-list 1	switch b result	
set metric 400	N E2 192.168.6.0/24	[2/400] tag: 0
!		via
route-map test3 permit 50	192.168.1.1, ethv0.1	
match ip address prefix-list 2	N E2 192.168.7.0/24	[2/600] tag: 0
set metric 600		via
!	192.168.1.1, ethv0.1	

#### 14.6.5 Filter Routing Using Prefix Lists

Methods of OSPF filtering LSA: area filter-list prefix; **Only those three types of LSA produced from the ABR can be filtered.**

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>router ospf</b>	Enter the OSPF configuration mode.
Step 3	<b>area <i>area-id</i> filter-list prefix &lt;prefix&gt;</b> ( <i>in out</i> )	Configure the list of prefixes within the region.
Step 4	<b>exit</b>	Return to privileged EXEC mode.

Filter three types of LSA on ABR.

By default, R3 can learn the inter-area routes of 1.1.1.1, 11.11.11.11, 2.2.2.2, and 192.168.12.0. These routes are calculated by R3, which collects and calculates "three LSA classes injected from R2 into area0".

So what if we don't want R3 to learn the 11.11.11.11/32 route?

```
ip prefix-list 100 deny 11.11.11.11/32
ip prefix-list 100 permit 0.0.0.0/0 le 32
!
router ospf
```

area 0 filter-list prefix 100 in

The above command means that the prefix list filter is executed when three classes of LSA are injected from other regions into the area0 region. If it's area1 filter-list prefix 100 out, this command means to perform the prefix filter when injecting 3 classes of LSA from area1 into all other areas.

Note that when we deploy on ABR filtering scheme of this three kinds of LSA, able to filter only those generated from the three kinds of ABR LSA, above area0 by default in the flood of 1.1.1.1, 11.11.11.11, 2.2.2.2, 192.168.12.0 routing of these three kind of LSA are produced from R2, so can be filtered by prefix list.

## 15. DHCP Management Configuration

### 15.1 Configure DHCP server

Now, larger and larger number of IP address are needed to allocate. DHCP (Dynamic Host configuration Protocol) is created to solve this problem. It includes DHCP Server and DHCP Client. Requested by client, IP address are allocated by the server. Configure DHCP Server as the following table show:

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>config terminal</b>	Enter global configuration mode.
<b>Step 2a</b>	<b>dhcp-server [enable   disable]</b>	Disable the DHCP server function
<b>Step 2b</b>	<b>dhcp-server   dns1   dns2   dns3   wins]</b> <b>&lt;A.B.C.D&gt;</b>	Configure DHCP's DNS and WINS Server
<b>Step 2c</b>	<b>dhcp-server startip A.B.C.D endip</b> <b>A.B.C.D</b>	Configure DHCP IP address pool
<b>Step 2d</b>	<b>dhcp-server subnet A.B.C.D</b>	Configure DHCP mask
<b>Step 2e</b>	<b>dhcp-server gateway A.B.C.D</b>	Configure DHCP gateway
<b>Step 2f</b>	<b>dhcp-server interface vlan &lt;1-4095&gt;</b>	Add the VLAN to the DHCP Server (If want DHCP server successful, need to configure the vlan interface IP address)
<b>Step 2g</b>	<b>dhcp-server leasetime leasetime</b>	Configure IP address leasetime
<b>Step 3a</b>	<b>show dhcp-server</b>	Show DHCP server configuration
<b>Step 3d</b>	<b>show dhcp-server lease</b>	Show DHCP Server allocate IP address
<b>Step 4</b>	<b>copy running-config startup-config</b>	Save the configuration

### 15.2 Configure DHCP relay

Because the DHCP receiving need to broadcast, so the server and the client should be in the same network. The DHCP relay can save this issue effectively. Configure DHCP relay as the following table show:

1. Single DHCP relay configuration:

	<b>Command</b>	<b>Function</b>
Step 1	<b>config terminal</b>	Enter global configuration mode.
Step 2	<b>interface vlan <i>vlan_id</i></b>	Add VLAN and enter VLAN interface configuration <i>vlan_id</i> (1–4094);
Step 3	<b>dhcp relay A.B.C.D</b>	Configure the DHCP relay server IP address, and enable the DHCP relay
Step 3b	<b>no dhcp relay A.B.C.D</b>	Delete DHCP relay
Step 4	<b>exit</b>	Exit to global configuration mode
Step 5	<b>show dhcp-relay configure</b>	Show the DHCP relay configuration.
Step 6	<b>copy running-config startup-config</b>	Save the configuration

2. Multiple DHCP relay configuration:

	<b>Command</b>	<b>Function</b>
Step 1	<b>config terminal</b>	Enter global configuration mode.
Step 2	<b>dhcp-server group&lt;groupname&gt;</b>	Add a DHCP server group, and enter group configuration mode.
Step 3a	<b>dhcp-server A.B.C.D</b>	Add the DHCP server to the group.
Step 3b	<b>no dhcp-server A.B.C.D</b>	Delete DHCP server
Step 4	<b>exit</b>	Exit to the global configuration mode
Step 5	<b>interface vlan <i>vlan_id</i></b>	Add a VLAN and enter to VLAN interface configuration <i>vlan_id</i> (1–4094);
Step 6a	<b>dhcp relay server-select&lt;groupname&gt;</b>	Select DHCP server group.
Step 6b	<b>no dhcp relay server-select&lt;groupname&gt;</b>	Delete the DHCP server group.
Step 7	<b>exit</b>	Exit to global configuration mode
Step 8	<b>show dhcp-relay configure</b>	Show DHCP relay configuration.
Step 9	<b>copy running-config startup-config</b>	Save the configuration.

## 15.3 Configure DHCP Snooping

To prevent the DHCP message attacking and protect you network to get a useful IP address. DHCP Snooping is used for do that. Configure DHCP Snooping as the following table show:

### A. DHCP Snooping enable/disable

	Command	Function
Step 1	<b>config terminal</b>	Enter global configuration mode.
Step 2	<b>dhcp-snooping (enable disable)</b>	Enable/disable DHCP Snooping. (DHCP Snooping enable, can not open dhcp server and dhcp relay)
Step 3a	<b>dhcp-snooping vlan &lt;1-4095&gt;...</b>	Configure DHCP Snooping vlan list
Step 3b	<b>nodhcp-snooping vlan &lt;1-4095&gt;...</b>	Delete DHCP Snooping vlan list
Step 4	<b>exit</b>	Exit to global configuration mode.
Step 5	<b>show dhcp-snooping configuration</b>	Show DHCP Snooping configuration.
Step 6	<b>copy running-config startup-config</b>	Save configuration.

### B. Configure DHCP Snooping option82

	Command	Function
Step 1	<b>config terminal</b>	Enter global configuration mode.
Step 2	<b>dhcp-snooping information option (enable disable)</b>	Enable/disable DHCP Snooping option82.
Step 3	<b>dhcp-snooping information strategy (drop keep release)</b>	Deal with the message with option82, drop、keep and replace.
Step 4	<b>exit</b>	Exit to global configuration mode.
Step 5	<b>show dhcp-snooping configuration</b>	Show DHCP Snooping configuration.
Step 6	<b>copy running-config startup-config</b>	Save configuration.

### C. Configure DHCP Snooping binding list

	Command	Function
Step 1	<b>config terminal</b>	Enter global configuration mode.

Step 2	<b>dhcp-snooping binding</b> <b>HHHH:HHHH:HHHH vlan &lt;1-4095&gt;</b> <b>A.B.C.D interface {interface_type</b> <b>slot/port} lease &lt;60-1000000&gt;</b>	Add the static DHCP binding list.
	<b>no dhcp-snooping binding</b> <b>HHHH:HHHH:HHHH</b>	Delete MAC binding list.
	<b>no dhcp-snooping binding</b> <b>(all static dynamic)</b>	Delete DHCP binding list.can delete all、static、dynamic .
Step 3	<b>dhcp-snooping binding</b> <b>delete-time&lt;1-3600&gt;</b>	Configure the biding list aging time and delete time.
Step 4	<b>exit</b>	Exit to global configuration mode
Step 5	<b>show dhcp-snooping configuration</b>	Show DHCP Snooping configuration.
Step 6	<b>copy running-config startup-config</b>	Save configuration.

## D.Configure DHCP Snooping port

	<b>Command</b>	<b>Function</b>
Step 1	<b>config terminal</b>	Enter global configuration mode.
Step 2	<b>interface {interface_type slot/port}</b>	Enter the interface configuration
Step 3a	<b>dhcp-snooping (trust untrust)</b>	Configure the trust/untrust port. All the port are untrust in default.
Step 3b	<b>dhcp-snooping information circuit-id</b> <b>string &lt;string&gt;</b>	Configure the option82的circuit-id value.
Step 3c	<b>no dhcp-snooping information circuit-id</b> <b>string &lt;string&gt;</b>	Delete the option82 circuit-id value , and load default.
Step 3d	<b>dhcp-snooping information remote-id</b> <b>string &lt;string&gt;</b>	Configure option82remote-id value.
Step 3e	<b>no dhcp-snooping information</b> <b>remote-idstring &lt;string&gt;</b>	Delete option82 remote-id value, load default value.
Step 3f	<b>dhcp-snooping limit rate&lt;0-4096&gt;</b>	Configure the port max speed of receiving the DHCP packet. It

		doesn't limit by default.
<b>Step 3e</b>	<b>no dhcp-snooping limit rate</b>	No limit speed.
<b>Step 4</b>	<b>exit</b>	Exit to the global configuration mode
<b>Step 5a</b>	<b>dhcp-snooping errdisable recovery (enable disable)</b>	Configure whether the port get down when the DHCP packetreceiving speed larger then the limit speed .The default is disable.
<b>Step 5b</b>	<b>dhcp-snooping errdisable recoveryinterval&lt;3-3600&gt;</b>	Configure the time when the port recovery after getting down
<b>Step 6</b>	<b>show dhcp-snooping configuration</b>	Show DHCP Snooping configuration.
<b>Step 7</b>	<b>copy running-config startup-config</b>	Save configuration.

## 15.4 Configuring IP Source Guard

### 15.4.1 Understanding IP Source Guard

IPSG is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database and on manually configured IP source bindings. You can use IP source guard to prevent traffic attacks if a host tries to use the IP address of its neighbor. You can enable IP source guard when DHCP snooping is enabled on an untrusted interface. After IPSG is enabled on an interface, the switch blocks all IP traffic received on the interface except for DHCP packets allowed by DHCP snooping. A port access control list (ACL) is applied to the interface. The port ACL allows only IP traffic with a source IP address in the IP source binding table and denies all other traffic.

Note:The port ACL takes precedence over any router ACLs or VLAN maps that affect the same interface.

The IP source binding table bindings are learned by DHCP snooping or are manually configured (static IP source bindings). An entry in this table has an IP address with its associated MAC address and VLAN number. The switch uses the IP source binding table only when IP source guard is enabled.

IPSG is supported only on Layer 2 ports, including access and trunk ports.You can configure IPSG with source IP address filtering or with source IP and MAC address filtering.

#### 15.4.1.1 Source IP Address Filtering

When IPSG is enabled with this option, IP traffic is filtered based on the source IP address. The switch forwards IP traffic when the source IP address matches an entry in the DHCP snooping binding database or a binding in the IP source binding table.

When a DHCP snooping binding or static IP source binding is added, changed, or deleted on an interface, the switch modifies the port ACL using the IP source binding changes, and re-applies the port ACL to the interface.

If you enable IP source guard on an interface on which IP source bindings (dynamically learned by DHCP snooping or manually configured) are not configured, the switch creates and applies a port ACL that denies all IP traffic on the interface. If you disable IP source guard, the switch removes the port ACL from the interface.

### 15.4.1.2 Source IP and MAC Address Filtering

IP traffic is filtered based on the source IP and MAC addresses. The switch forwards traffic only when the source IP and MAC addresses match an entry in the IP source binding table.

When address filtering is enabled, the switch filters IP and non-IP traffic. If the source MAC address of an IP or non-IP packet matches a valid IP source binding, the switch forwards the packet. The switch drops all other types of packets except DHCP packets.

The switch uses port security to filter source MAC addresses. The interface can shut down when a port-security violation occurs.

### 15.4.1.3 IP Source Guard for Static Hosts

Note: Do not use IPSG for static hosts on uplink ports or trunk ports.

IPSG for static hosts extends the IPSG capability to non-DHCP and static environments. The previous IPSG used the entries created by DHCP snooping to validate the hosts connected to a switch. Any traffic received from a host without a valid DHCP binding entry is dropped. This security feature restricts IP traffic on nonrouted Layer 2 interfaces. It filters traffic based on the DHCP snooping binding database and on manually configured IP source bindings. The previous version of IPSG required a DHCP environment for IPSG to work.

IPSG for static hosts allows IPSG to work without DHCP. IPSG for static hosts relies on IP device tracking-table entries to install port ACLs. The switch creates static entries based on ARP requests or other IP packets to maintain the list of valid hosts for a given port. You can also specify the number of hosts allowed to send traffic to a given port. This is equivalent to port security at Layer 3.

IPSG for static hosts initially learns IP or MAC bindings dynamically through an ACL-based snooping mechanism. IP or MAC bindings are learned from static hosts by ARP and IP packets. They are stored in the device tracking database. When the number of IP addresses that have been dynamically learned or statically configured on a given port reaches a maximum, the hardware drops any packet with a new IP address.

## 15.4.2 Configuring IP Source Guard

### 15.4.2.1 Default IP Source Guard Configuration

By default, IP source guard is disabled.

### 15.4.2.2 IP Source Guard Configuration Guidelines

- You can configure static IP bindings only on nonrouted ports. If you enter the `ip source binding mac-address vlan vlan-id ip-address interface interface-id global configuration` command on a routed interface, this error message appears: Static IP source binding can only be configured on switch port.
- When IP source guard with source IP filtering is enabled on an interface, DHCP snooping must be enabled on the access VLAN for that interface.
- If you are enabling IP source guard on a trunk interface with multiple VLANs and DHCP snooping is enabled on all the VLANs, the source IP address filter is applied on all the VLANs.

Note: If IP source guard is enabled and you enable or disable DHCP snooping on a VLAN on the trunk interface, the switch might not properly filter traffic.

- If you enable IP source guard with source IP and MAC address filtering, DHCP snooping and port security must be enabled on the interface. You must also enter the `ip dhcp snooping information option global configuration` command and ensure that the DHCP server supports option 82. When IP source guard is enabled with MAC address filtering, the DHCP host MAC address is not learned until the host is granted a lease. When forwarding packets from the server to the host, DHCP snooping uses option-82 data to identify the host port.
- When configuring IP source guard on interfaces on which a private VLAN is configured, port security is not supported.
- IP source guard is not supported on EtherChannels.
- You can enable this feature when IEEE 802.1x port-based authentication is enabled.
- If the number of ternary content addressable memory (TCAM) entries exceeds the maximum available, the CPU usage increases.

### 15.4.2.3 Enabling IP Source Guard

Begin at privileged configuration mode, follow these steps to enable and configure IP source guard on an interface.

Note:

1. you can define static binding list.

2. system will auto syn the dhcp-snooping binding list. when you enable dhcp-snooping.

	Command	Function
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>interface interface_type slot/port</code>	Enter interface configuration mode, and specify the interface to be configured.
Step 3	<code>ip verify source ip-address</code>	• Enable IP source guard with source IP

	or <b>ip verify source mac-address</b> or <b>ip verify source ip-mac-address</b>	address filtering. • Enable IP source guard with source MAC address filtering. • Enable IP source guard with source IP and MAC address filtering.
<b>Step 4</b>	<b>exit</b>	Return to global configuration mode.
<b>Step 5</b>	<b>ip source binding</b> <i>mac-address</i> <b>vlan</b> <i>vlan-id ip-address</i> <b>interface</b> <i>interface_type slot/port</i>	Add a static IP source binding. Enter this command for each static binding.
<b>Step 6</b>	<b>show ip verify source</b> [ <b>interface</b> <i>interface_type slot/port</i> ]	Verify the IP source guard configuration.
<b>Step 7</b>	<b>show ip source binding</b>	Display the IP source bindings on the switch, on a specific VLAN, or on a specific interface.
<b>Step 8</b>	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To disable IP source guard with source IP address filtering, use the **no ip verify source** interface configuration command.

To delete a static IP source binding entry, use the **no ip source global** configuration command.

### 15.4.3 Configuring IP Source Guard for Static Hosts on a Layer 2 Access Port

Begin at privileged configuration mode:

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface</b> <i>interface_type slot/port</i>	Enter interface configuration mode, and specify the interface to be configured.
<b>Step 3</b>	<b>switchport mode access</b>	Configure a port as access.
<b>Step 4</b>	<b>switchport access vlan</b> <i>vlan-id</i>	Configure the VLAN for this port.
<b>Step 5</b>	<b>ip verify source ip-mac-address</b>	Enable IPSG for static hosts with MAC address filtering.
<b>Step 6</b>	<b>end</b>	Return to privileged EXEC mode.
<b>Step 7</b>	<b>show ip verify source interface</b> <i>interface_type slot/port</i>	Verify the configuration and display IPSG permit ACLs for static hosts.



## 16. IPv6

### 16.1 VLAN IPv6 Address

#### 16.1.1 Configure/delete VLAN IPv6 address

	Command	Function
Step 1	<b>config terminal</b>	Enter global configuration mode.
Step 2	<b>interface vlan</b> <i>vlan_id</i>	enter VLAN interface configuration <i>vlan_id</i> range:1~4094
Step 3a	<b>ipv6 address</b> <X:X::X:X/M> <i>[eui-64]</i>	Configure the IPv6 address and prefix length of the vlan interface. By default, the interface automatically generates a link-local address. Eui-64, which is an optional parameter, is used to automatically fill the low 64-bit of IPv6 address according to the eui-64 specification.
Step 3b	<b>ipv6 address</b> <X:X::X:X> <i>link-local</i>	Configure the IPv6 link-local address of the vlan interface.
	<b>no ipv6 address</b> <X:X::X:X/M>	Delete specified IPv6 address of VLAN interface.
	<b>no ipv6 address</b>	Delete all IPv6 addresses of the VLAN interface.
Step 4	<b>no ipv6 address</b> <X:X::X:X> <i>link-local</i>	Restore the default link-local address of VLAN interface.
	<b>exit</b>	Exit to global configuration mode.
Step 5	<b>show interface vlan</b> <i>vlan_id</i>	Verify the configuration information.
Step 6	<b>write</b>	Save configurations.

### 16.2 IPv6 Static Neighbour

The neighbor items are the neighbor information of the device in the link range. The device neighbor items can be created dynamically through the neighbor request message NS

and the neighbor advertisement message NA; it also can be created manually.

The device identifies a static neighbor item uniquely based on the IPv6 address of the neighboring node and the interface number that connected to the neighboring node.

When you delete a static neighbor item corresponding to a VLAN interface, you only need to specify the VLAN interface.

	Command	Function
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>ipv6 neighbor &lt;X:X::X:X&gt; vlan vlan_id &lt;HHHH: HHHH:HHHH&gt;</b>	Add a static item to the neighbor discovery table, you must specify the network interface and link layer address.
<b>Step 3</b>	<b>no ipv6 neighbor &lt;X:X::X:X&gt; vlan vlan_id</b>	Delete the specified item of the neighbor discovery table.
<b>Step 4</b>	<b>show ipv6 neighbors</b>	Show the neighbor items in the current neighbor discovery table.

## 16.3 IPv6 SLAAC

An IPv6 address consists of two parts: prefix and interface ID. A big feature of IPv6 is that it supports plug and play. IPv6 address stateless autoconfiguration means that the node configures an IPv6 address automatically based on the information assigned by the router discovery/prefix discovery. Router discovery/prefix discovery means that when a node is connected to an IPv6 link, it can discover the local router, obtain the prefix of the neighbor router and its network, and other configuration parameters from the received RA message without With the Dynamic Host Configuration Protocol (DHCPv6).

The device can obtain the IPv6 address prefix which carried in the RA message (Router-Advertisement, ICMPv6 Type 134), and generate the interface ID automatically through the interface, so as to get a completed 128-bit IPv6 address. By default, the RA message is sent once every 600s. The device can also send an RS (router solicit, ICMPv6 Type = 133) message to obtain the prefix.

Parameter Discovery: A node can discover the parameters of the link it is connected to, such as the MTU of the link and the hop limit.

### 16.3.1 IPv6 SLAAC Work processes

The router discovery/prefix discovery is implemented by router solicitation message RS and router advertisement message RA. The specific process is as follows:

- (1) When the node starts up, it sends a request to the router through RS message, requesting the prefix and other configuration information for the configuration of the node.
- (2) The router responds a RA message, which includes the prefix information option (the router also sends the RA message periodically). The prefix information option includes not only the prefix information of IPv6 address but also the preferred lifetime and valid lifetime

of the prefix. After receiving the periodical RA message, the node will update the preferred lifetime and valid lifetime of the prefix based on the message.

(3) The node configures IPv6 address and other information of the interface automatically by using the prefix and other configuration parameters in the RA message responded by the router. During the valid lifetime, the automatically generated address can be used normally; after the valid lifetime expired, the automatically generated address will be deleted.

### 16.3.2 IPv6 SLAAC Configuration

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface vlan <i>vlan_id</i></b>	Enter VLAN interface configuration. <i>vlan_id</i> range: 1—4094.
Step 3	<b>no ipv6 nd suppress-ra</b>	Disable RA message suppression. The interface sends RA messages periodically (default 600S). By default, RA message suppression is enabled.
Step 4a	<b>ipv6 nd suppress-ra</b>	Enable RA message suppression.
Step 4b	<b>ipv6 nd ra-interval &lt;1-1800&gt;</b>	Configure the interval for sending RA messages in second. The minimum value is 1s and the maximum value is 1800s. The default is 600s.
Step 5	<b>ipv6 nd ra-lifetime &lt;0-9000&gt;</b>	Configure the lifetime of the RA message. The minimum value is 0s and the maximum value is 9000s. The default is 1800s.
Step 6	<b>ipv6 nd reachable-time &lt;1-3600000&gt;</b>	Specify the reachability interval of a new neighbor. It is used to detect neighbors that are unreachable in the neighbor discovery table. The minimum value is 1s and the maximum value is 3600000s. The default is 0s.
Step 7	<b>ipv6 nd home-agent-config-flag</b>	The set/unset flag in IPv6 router advertisement message is used to

		indicate to the host that the router acts as a home agent and includes the home agent option. It is not set by default.
<b>Step 8</b>	<b>ipv6 nd home-agent-preference</b> <0-65535>	When the local proxy configuration flag is set, this value indicates the host proxy preference. The default value 0 indicates the lowest priority.
<b>Step 9</b>	<b>ipv6 nd home-agent-lifetime</b> <0-65520>	When the local proxy configuration flag is set, this value indicates the host agent lifetime. The default value is 0.
<b>Step 10</b>	<b>ipv6 nd adv-interval-option</b>	Advertisement Interval option indicates the maximum time (in milliseconds) between consecutive unsolicited router advertisements.
<b>Step 11</b>	<b>ipv6 nd managed-config-flag</b>	This flag bit indicates which automatic configuration mode is used to obtain the IPv6 address. When the M bit is set to 1, the device that received the RA message will use the configuration protocol (such as DHCPv6) to obtain an IPv6 address. By default, this flag bit is 0.
<b>Step 12</b>	<b>ipv6 nd other-config-flag</b>	This flag bit indicates which mode is used to configure other configuration information (such as DNS, domain name, etc.) except IPv6 address. When the O bit is set to 1, the device that received this RA message will use the configuration protocol (such as DHCPv6) to obtain configuration information except IPv6 address. By default, this flag bit is 0.
<b>Step 13</b>	<b>ipv6 nd prefix</b> <X:X::X:X/M> [valid-lifetime][ preferred-lifetime] [off-link] [no-autoconfig] [router-address]	Configure the parameters of the prefix declared on the network interface; <b>Valid-lifetime:</b> The length of time (in seconds) that the prefix is valid. The value infinite means infinity. Range: <0-4294967295 infinite> Default: 2592000 <b>Preferred-lifetime:</b> The preferred length of time (in seconds) for the prefix. Range: <0-4294967295 infinite> Default: 604800

		<p><b>off-link:</b> Indicates that the link or link attribute does not declare a prefix.</p> <p><b>no-autoconfig:</b> Indicates to the device on the link that the specified prefix cannot be used for IPv6 autoconfiguration.</p> <p><b>router-address:</b> The R flag indicates to the host on the local link that the specified prefix contains the full IPv6 address.</p>
<b>Step 14</b>	<b>ipv6 nd router-preference (high medium low)</b>	Set router preferences.
<b>Step 15</b>	<b>ipv6 nd mtu &lt;1-65535&gt;</b>	Configure the interface MTU. MTU range: 1-65535. The default is 0.

### 16.3.3 Example(pending)

## 16.4 DHCPv6

### 16.4.1 DHCPv6 overview

DHCPv6 (Dynamic Host Configuration Protocol for IPv6) is a protocol designed for IPv6 addressing schemes that assigns IPv6 prefixes, IPv6 addresses, and other network configuration parameters to hosts.

Compared with other IPv6 address allocation methods (manual configuration, stateless autoconfiguration through network prefix in router advertisement messages, etc.), DHCPv6 has the following advantages:

- Not only IPv6 addresses, but also IPv6 prefixes can be assigned to facilitate automatic configuration and management of the whole network.
- Better control of address allocation. Not only can DHCPv6 record the address/prefix assigned to the host, but it can also assign a specific address/prefix to a specific host for network management.
- In addition to the IPv6 prefix and IPv6 address, it can also assign network configuration parameters such as DNS server and domain name to the host.

#### 16.4.1.1 DHCPv6 network composition

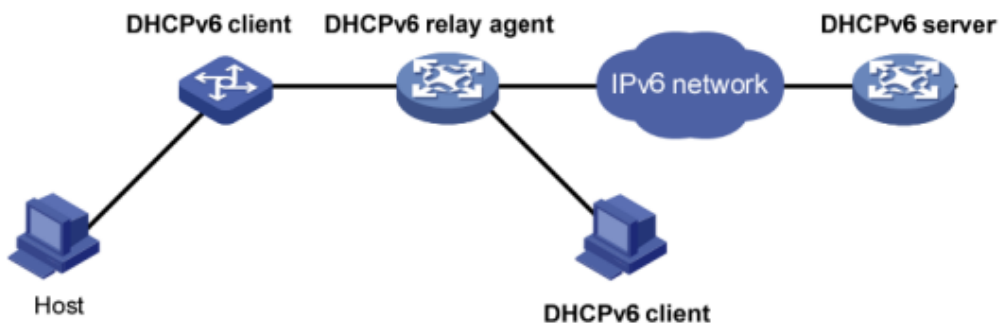


Figure 1: DHCPv6 network Composition

As shown in figure 1, the DHCPv6 networking includes the following three roles:

□

**DHCPv6 client:** A device that dynamically obtains IPv6 addresses, IPv6 prefixes, or other network configuration parameters. □

**DHCPv6 server:** A device responsible for assigning IPv6 addresses, IPv6 prefixes, and other network configuration parameters to DHCPv6 clients. A DHCPv6 server can not only assign an IPv6 address to a DHCPv6 client, but also assign an IPv6 prefix to it. As shown in figure 1, after the DHCPv6 server assigns an IPv6 prefix to the DHCPv6 client, the DHCPv6 client sends an RA message containing the prefix information to the network, so that hosts on the network automatically configure an IPv6 address based on the prefix. □

**DHCPv6 relay:** The DHCPv6 client communicates with the DHCPv6 server through the link-local multicast address to obtain IPv6 addresses and other network configuration parameters. If the server and the client are not on the same link, you need to forward packets through the DHCPv6 relay. This prevents the DHCPv6 server from being deployed on each link. This saves costs and facilitates centralized management.

#### 16.4.1.2 DHCPv6 DUID configuration

The server uses the DUID (DHCP Unique Identifier) to identify different clients, and the client uses the DUID to identify the server. The contents of the client and server DUID are carried in the Client Identifier and Server Identifier options in the DHCPv6 message. The format of the two options is the same. The value of the option-code field is used to distinguish between the Client Identifier and the Server Identifier option.

The minimum length is 12 bytes (96 bits) and the maximum length is 20 bytes (160 bits). The actual length depends on its type. The server compares the DUID to its database and sends the configuration data (address, lease, DNS server, etc.) to the client.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>duid</b> { <b>duid-llt duid-ll duid-en</b> <b>&lt;1-4294967295&gt;  duid-uuid &lt;word&gt;</b> }	Configure DUID.
Step 3	<b>show ipv6 dhcp duid</b>	Display DUID configuration.
Step 4	<b>write</b>	Save configuration.

## 16.4.2 DHCPv6 Server

### 16.4.2.1 DHCPv6 address/prefix allocation process

The process of assigning addresses/prefixes to clients by the DHCPv6 server is divided into two categories:

- Quickly allocation process with two messages exchanging.
- Allocation process with four messages exchanging.

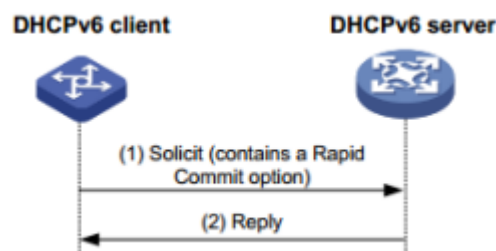


Figure 2: Quickly allocation process with two messages exchanging

As shown in figure 2, the address/prefix quick assignment process is:

(1) The DHCPv6 client carries the Rapid Commit option in the sent Solicit message, indicating that the client wants the server to quickly assign an address/prefix and network configuration parameters to it;

(2) If the DHCPv6 server supports the fast allocation process, it directly returns a Reply message to assign the IPv6 address/prefix and other network configuration parameters to the client. If the DHCPv6 server does not support the fast assignment process, the client is assigned an IPv6 address/prefix and other network configuration parameters using an assignment process that interacts with four messages.

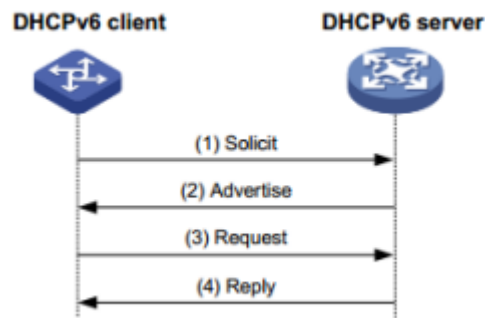


Figure 3: Allocation process with four messages exchanging

Step	Message type	Description
(1)	Solicit	The DHCPv6 client sends the message requesting the DHCPv6 server to assign an IPv6 address/prefix and network configuration parameters to it.
(2)	Advertise	If the Rapid Commit option is not carried in the Solicit message, or the Rapid Commit option is carried in the Solicit message, but the server does not support the fast allocation process, the DHCPv6 server replies to the message, notifying the client of the address/prefix and network configuration parameters that can be assigned to it.
(3)	Request	If the DHCPv6 client receives Advertise messages from multiple servers, it selects one of the servers according to the order in which the messages are received, the server priority, etc., and sends a Request message to the server, requesting the server to confirm the address/prefix. And network configuration parameters
(4)	Reply	The DHCPv6 server replies to the message, confirming that the address/prefix and network configuration parameters are assigned to the client.

#### 16.4.2.2 DHCPv6 Server lease renewal process

The IPv6 address/prefix assigned to the client by the DHCPv6 server has a certain lease term. The rental period is determined by the valid life period (Valid Lifetime). After the lease time of the address/prefix reaches the valid lifetime, the DHCPv6 client can no longer use the address/prefix. If the DHCPv6 client wishes to continue using the address/prefix before the valid lifetime expires, the address/prefix lease needs to be updated.

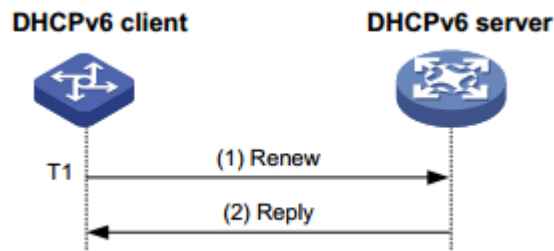


Figure 4: Update address/prefix lease by renew

As shown in Figure 4, when the address/prefix lease time arrival time T1 (the recommended value is half of the preferred lifetime Preferred Lifetime), the DHCPv6 client unicasts the Renew message to the DHCPv6 server that assigns the address/prefix to it. Update the address/prefix lease. If the client can continue to use the address/prefix, the DHCPv6 server responds with a successful Reply packet, informing the DHCPv6 client that the address/prefix lease has been successfully updated; if the address/prefix cannot be reassigned to the client, The DHCPv6 server responds with a Reply packet that failed to renew, notifying the client that it cannot obtain a new lease.

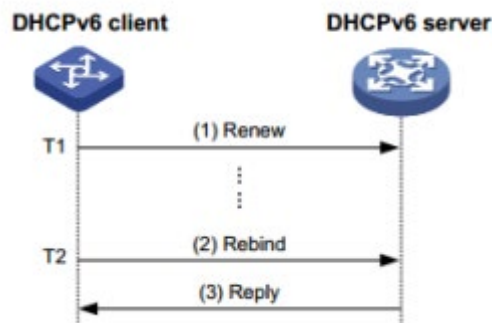


Figure 5: Update address/prefix lease by rebind

As shown in Figure 5, if Renew is sent to update the lease at T1, but the response packet from the DHCPv6 server is not received, the DHCPv6 client will send all DHCPv6 to T2 (recommended value is 0.8 times of the preferred lifetime). The server multicasts the Rebind message and requests to update the lease. If the client can continue to use the address/prefix, the DHCPv6 server responds with a successful Reply message, informing the DHCPv6 client that the address/prefix lease has been successfully updated; if the address/prefix cannot be reassigned to the client, The DHCPv6 server responds to the Reply packet with the renewal failure, notifying the client that the new lease cannot be obtained. If the DHCPv6 client does not receive the response packet from the server, the client stops using the address/prefix after the valid lifetime expires.

### 16.4.2.3 DHCPv6 Server stateless configuration

The DHCPv6 server can assign additional network configuration parameters to clients that already have an IPv6 address/prefix. This process is called a DHCPv6 stateless configuration.

After the DHCPv6 client successfully obtains an IPv6 address through the stateless

auto-configuration function, the M flag (Managed address configuration flag) in the RA (Router Advertisement, Router Advertisement) packet is 0. If the other stateful configuration flag (1), the DHCPv6 client automatically starts the DHCPv6 stateless configuration function to obtain other network configuration parameters except the address/prefix.

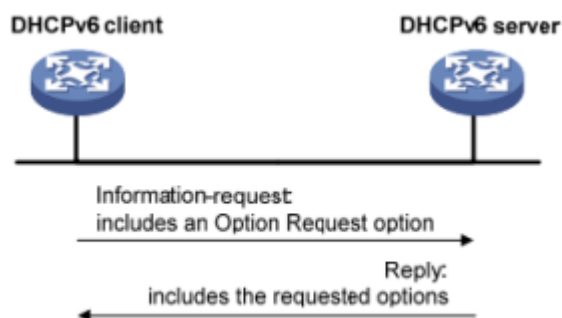


Figure 6: DHCPv6 stateless configuration process

As shown in Example 6, the specific process of DHCPv6 stateless configuration is as follows:

(1) The client sends an Information-request packet to the DHCPv6 server in multicast mode. The packet carries the Option Request option to specify the configuration parameters that the client needs to obtain from the server.

(2) After receiving the Information-request packet, the server allocates network configuration parameters to the client and sends a Reply packet to the client to return the network configuration parameters to the client.

(3) The client provides the information provided in the Reply packet. If the configuration parameter is the same as the one specified in the Reply message, the network configuration is performed according to the parameters provided in the Reply packet. Otherwise, the parameter is ignored. If multiple Reply packets are received, the client selects the first reply packet and completes the stateless configuration of the client according to the parameters provided in the packet.

#### 16.4.2.4 DHCPv6 Server configurations

Begin at privileged configuration mode, configure DHCPv6 server as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ipv6 dhcp pool</b> <i>pool_name</i>	Configure an IPv6 DHCP address pool.
Step 3	<b>prefix-delegation</b> <X:X::X:X/M> <X:X::X:X/M> [ <b>lifetime</b>	Configure prefix-delegation and its lifetime.

	<60-4294967295 infinite> <60-4294967295 infinite>]	
Step 4	<b>address prefix</b> <X:X::X:X/M> <b>[lifetime</b> <60-4294967295 infinite> <60-4294967295 infinite>]	Configure IPv6 address prefix and its lifetime.
Step 5	<b>dns-server</b> <X:X::X:X>	Configure the DNS server IPv6 address.
Step 6	<b>domain-name</b> <WORD>	Configure domain name.
Step 7	<b>nis address</b> <X:X::X:X>	Configuring the NIS server IPv6 address.
Step 8	<b>nis domain-name</b> <WORD>	Configuring the NIS server domain name.
Step 9	<b>nisp address</b> <X:X::X:X>	Configure the NISP server IPv6 address.
Step 10	<b>nisp domain-name</b> <WORD>	Configure the NISP server domain name.
Step 11	<b>ntp address</b> <X:X::X:X>	Configure the NTP server IPv6 address.
Step 12	<b>sip address</b> <X:X::X:X>	Configure the SIP server IPv6 address.
Step 13	<b>sip domain-name</b> <WORD>	Configure the SIP server domain name.
Step 14	<b>bcmcs address</b> <X:X::X:X>	Configuring the BCMCS server IPv6 address.
Step 15	<b>bcmcs domain-name</b> <WORD>	Configure the BCMCS server domain name.
Step 16	<b>exit</b>	Exit to global configuration mode.
Step 17	<b>interface vlan</b> <i>vlan_id</i>	Add VLAN and enter VLAN interface configuration. <i>vlan_id</i> (1–4094);
Step 18	<b>ipv6 dhcp server</b> <i>pool_name</i> <b>[preference</b> <0-255 >] <b>[allow-hint] [rapid-commit]</b>	Configure and enable the DHCPv6 server address of the network segment on the interface.
Step 19	<b>exit</b>	Exit to global configuration mode.
Step 20	<b>show ipv6 dhcp pool</b>	View DHCPv6 address pool information..
Step 21	<b>show ipv6 dhcp interface</b> [ <b>vlan</b> <1-4094>]	Show information about the device DHCPv6 interface

<b>Step 22</b>	<b>show ipv6 dhcp binding</b>	View the address binding information of the DHCPv6 address pool.
<b>Step 23</b>	<b>write</b>	Save configurations.

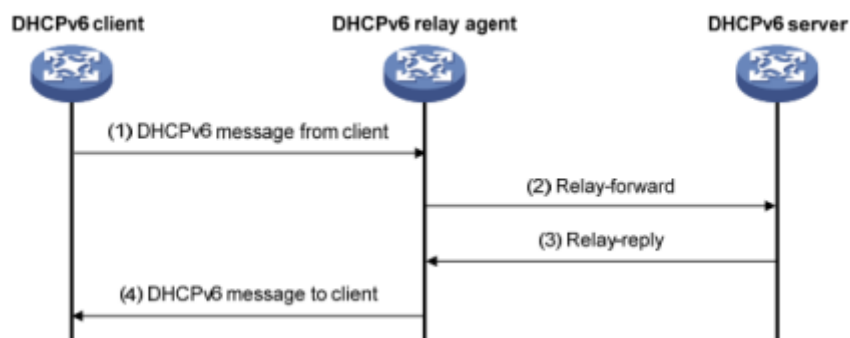
### 16.4.2.5 Example(pending)

## 16.4.3 DHCPv6 Relay

### 16.4.3.1 DHCPv6 Relay work processes

During the process of obtaining the IPv6 address/prefix and other network configuration parameters dynamically through the DHCPv6 relay, the DHCPv6 client and the DHCPv6 server are processed in the same way as when the DHCPv6 relay is not processed.

DHCPv6 relay forwarding process:



(1) The DHCPv6 client sends a request to the multicast address FF02::1:2 of all DHCPv6 servers and relays;

(2) After receiving the request, the DHCPv6 relay encapsulates the relay-forward packet in the relay message option and sends the relay-forward packet to the DHCPv6 server.

(3) The DHCPv6 server parses the client's request from the relay-forward packet, selects the IPv6 address and other parameters for the client, constructs a response message, and encapsulates the response message in the relay message option of the Relay-reply message. Send the Relay-reply message to the DHCPv6 relay.

(4) The DHCPv6 relay resolves the response from the server to the DHCPv6 client from the relay-reply packet. The DHCPv6 client performs network configuration based on the IPv6 address/prefix and other parameters assigned by the DHCPv6 server.

### 16.4.3.2 DHCPv6 Relay configuration

Begin at privileged configuration mode, configure DHCPv6 relay as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface vlan <i>vlan_id</i></b>	Add VLAN and enter VLAN interface configuration <i>vlan_id</i> (1-4094);
Step 3	<b>ipv6 dhcp relay destination &lt;X:X::X:X&gt;</b>	Configure the DHCPv6 relay server address on the network segment of the interface and enable the DHCPv6 relay service.
Step 4	<b>exit</b>	Exit to global configuration mode.
Step 5	<b>show ipv6 dhcp interface</b>	Show information about the device DHCPv6 interface.
Step 6	<b>write</b>	Save configurations.

#### 16.4.3.3 DHCPv6 Relay Option 37 configuration

Begin at privileged configuration mode, configure DHCPv6 relay option 37 as the following table shows.

Step 1	<b>configure terminal</b>	Enter global configuration mode.
	<b>ipv6 dhcp relay remote-id option</b>	Enable relay support option 38 option function
Step 2	<b>interface vlan <i>vlan_id</i></b>	Add VLAN and enter VLAN interface configuration. <i>vlan_id</i> (1-4094);
Step 3	<b>ipv6 dhcp relay remote-id &lt;WORD&gt;</b>	Configure the remote-id value of the custom option37.
	<b>show ipv6 dhcp relay option</b>	Display configuration information about trunk related options.
Step 4	<b>exit</b>	Exit to global configuration mode.
Step 5	<b>write</b>	Save configurations.

#### 16.4.3.4 DHCPv6 Relay Option 38 configuration

Begin at privileged configuration mode, configure DHCPv6 relay option 38 as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
	<b>ipv6 dhcp relay subscriber-id option</b>	Enable relay support option 38 option function
<b>Step 2</b>	<b>interface vlan <i>vlan_id</i></b>	Add VLAN and enter VLAN interface configuration.vlan_id(1-4094);
<b>Step 3</b>	<b>ipv6 dhcp relay subscriber-id &lt;WORD&gt;</b>	Configure the custom subscriber-id value of option38.
	<b>show ipv6 dhcp relay option</b>	Display configuration information about trunk related options.
<b>Step 4</b>	<b>exit</b>	Exit to global configuration mode.
<b>Step 5</b>	<b>write</b>	Save configurations.

#### 16.4.3.5 Example(pending)

## 16.5 IPv6 Route

### 16.5.1 IPv6 static route configuration

#### IPv6 Static Routes Introduction

A static route is a special type of route that is manually configured by an administrator. When the network structure is relatively simple, you only need to configure a static route to make the network work normally. Static routes cannot automatically adapt to changes in network topology. After the network fails or the topology changes, the configuration must be manually modified by the network administrator. IPv6 static routes are similar to IPv4 static routes and are suitable for some IPv6 networks with simple structures.

#### Default Routes Introduction

The IPv6 default route is the route used when the router does not find a matching IPv6 routing entry. There are two ways to generate IPv6 default routes:

- The first type is manually configured by the network administrator. The function address specified during configuration is `::/0` (prefix length is 0).
- The second type is dynamic routing protocol generation (such as OSPFv3, IPv6 IS-IS, and RIPng). Routers with strong routing capabilities advertise IPv6 default routes to other routers. Other routers generate pointers to them in their routing tables. The default route of the router.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ipv6 route</b> <X:X::X:X/M> <X:X::X:X>	Add a static route.
Step 3	<b>no ipv6 route</b> <X:X::X:X/M> <X:X::X:X>	Delete static route.
Step 4	<b>show ipv6 route</b>	Show current routing configuration

### 16.5.2 View IPv6 hardware routing information

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2a	<b>show ipv6 l3 defip route</b>	View IPv6 hardware subnet routing information.
Step 2b	<b>show ipv6 l3 hostroute</b>	View IPv6 hardware host routing information.
Step 2c	<b>show l3 interface</b>	View interface information.

## 16.6 IPv6 Connectivity Test

Ping6 is mainly used to check network connectivity and host reachability for IPv6.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ping6</b> <X:X::X:X> [-i vlan <1-4094>] [-s <packetsize>]	Packetize: The length of the packet to be sent, in bytes. Ping the link local address to specify

	the interface.
--	----------------

## 17. PON Management Configuration

### 17.1 Enable/Disable PON

Begin at privileged configuration mode, enable or disable PON port as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3	<b>pon {enable disable}</b>	Enable or disable PON optical transceiver.
Step 4	<b>show pon info</b>	Show PON information.

### 17.2 PON downstream encryption

EPON system transmits data with broadcast mode. So hacker can get other customer's information easily. In order to improve security, system can encrypt the data by encryption algorithm. This OLT supports triple churning encryption function for downstream.

Every LLID has its own key for triple churning encryption function. Churning needs OLT to request updating key. Then OLT accomplishes triple churning with 3 bytes key which ONU provides. It will churn all the data frames and OAM frames. By default, PON downstream encryption is disabled.

Begin at privileged configuration mode, enable PON downstream encryption as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3a	<b>pon encryption triple-churningkey_timer &lt;774-786426&gt;</b>	Enable PON downstream encryption.
Step 3b	<b>no pon encryption</b>	Disable PON downstream encryption.
Step 4	<b>show pon encryption</b>	Show pon encryption configuration.

### 17.3 Configure maximum RTT

The main purpose of configuring maximum RTT is to make sure ONU which are in different distances with OLT can register successful. Different ONU has different physical distance with OLT. This will make message round-trip time changes in microsecond. In this case, if there is not enough time slot and messages which come from different ONU may arrive at OLT at the same time, confliction will turn up.

In order to avoid the confliction, EPON system adopts time label to measure distance, which is based on EPON system time label sync, by calculating difference value between received time label and local clock counter time label. RTT can adjust ONU transmit delay and reduce send window interval so that it can improve upstream channel usage.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
<b>Step 3a</b>	<b>pon max-rtt &lt;2000-32000&gt;</b>	Configure maximum RTT
<b>Step 3b</b>	<b>pon max-rtt default</b>	Reset RTT to default. Default value is 14500.
<b>Step 4</b>	<b>Show pon info</b>	Show current RTT configuration.

### 17.4 PON ONU laser detect

Enable to detect whether a ONU is laser on in a PON port.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
<b>Step 3a</b>	<b>pon laser-always-on detect</b>	Enable PON port laser detection

### 17.5 Show PON port statistics

Begin at privileged configuration mode, show PON port statistics as the following table shows.

<b>Command</b>	<b>Function</b>
----------------	-----------------

<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
<b>Step 3</b>	<b>show pon statistics</b>	Show PON port statistics.

## 17.6 Show optical module parameters and alarms

Optical module parameters contain transmit optical power, receive optical power, temperature, voltage and bias current. These 5 parameters decide whether the optical module can work normal or not. Any of them is abnormal may cause ONU deregister or lose packets.

Begin at privileged configuration mode, show PON port optical module parameters as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
<b>Step 3</b>	<b>show pon optical transceiver</b>	Show pon optical parameters.

## 18. ONU Management Configuration

### 18.1 ONU basic configuration

#### 18.1.1 Configure ONU authentication mode

By default, it is disabled for ONU MAC checking mechanism. All ONU can register freely. You can use command **onu auth-mode mac** to enable ONU MAC checking mechanism when MPCP registering.

Use command **onu auth-mode loid** to enable ONU LOID authentication mode. After registered, OLT will request ONU LOID for authentication.

Use command **onu auth-mode hybrid** to enable hybrid authentication mode. In this mode, OLT will authenticate ONU by MAC address firstly, if failed, authenticate ONU by LOID.

Use command **show onu auth-info** to show active ONU information, includes ONU ID, LLID, ONU status, MAC address, OAM status, distance, last register time, last deregister time, deregister reason, online time and so on.

Use command **show onu auto-find** to show inactive ONU information, includes LLID, MAC address, ONU status, last register time, last deregister time, offline time, and so on.

Begin at privileged configuration mode, configure ONU authentication mode as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3	<b>onu auth-mode {disable mac loid hybrid}</b>	Configure ONU authentication mode.
Step 4	<b>show onu auth-mode</b>	Show ONU authentication mode.
Step 5	<b>show onu auth-info</b>	Show authenticated ONU.
Step 6	<b>show onu auto-find</b>	Show registered but not authenticated ONU.

#### 18.1.2 Remove authorized ONU

Begin at privileged configuration mode, remove authorized ONU as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.

Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3	<b>no onuauth onuid &lt;onuid&gt;</b>	Remove authorized ONU.

### 18.1.3 Deregister or reset ONU

Deregistering ONU only makes ONU off line, but not delete and unauthorized it.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3a	<b>{deregister reset} onu auth onuid &lt;onuid&gt;</b>	Deregister or reset specific ONU.
Step 3b	<b>{deregister reset} onu auth all</b>	Deregister or reset all ONUs.

### 18.1.4 Configure ONU authorization MAC list

When ONU authorization mode is MAC\_auth, you must configure MAC list. Begin at privileged configuration mode, configure MAC list as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3a	<b>onu mac-auth {add del} &lt;xx:xx:xx:xx:xx:xx&gt;</b>	Add or delete MAC white list.
Step 3b	<b>onu black-mac-auth {add del} &lt;xx:xx:xx:xx:xx:xx&gt;</b>	Add or delete MAC black list.
Step 3c	<b>onu {mac-auth  black-mac-auth} clean</b>	Clean MAC white list or black list.
Step 4	<b>show onu mac-auth</b>	Show ONU MAC white list.
Step 5	<b>show onu black-mac-auth</b>	Show ONU MAC black list.

### 18.1.5 Configure ONU authorization LOID list

When ONU authorization mode is LOID\_auth, you must configure LOID list. Begin at privileged configuration mode, configure LOID list as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3	<b>onu loid-auth</b>	Add or delete LOID list.

	<b>{add del}&lt;loid&gt;[&lt;password&gt;]*1</b>	
<b>Step 4</b>	<b>onu loid-auth clean</b>	Clean LOID list.
<b>Step 5</b>	<b>show onu loid-auth</b>	Show onu LOID list.

### 18.1.6 Measure ONU distance

Use the following commands to measure authorized ONU distance.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon slot/port</b>	Enter PON interface configuration mode.
<b>Step 3</b>	<b>show onu&lt;onuid&gt;rtt</b>	Measure ONU distance.

### 18.1.7 Configure ONU description string

Begin at privileged configuration mode, configure ONU description string as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon slot/port</b>	Enter PON interface configuration mode.
<b>Step 3</b>	<b>onu&lt;onuid&gt;description&lt;string&gt;</b>	Add description string to ONU.
<b>Step 4</b>	<b>show onu&lt;onuid&gt;description</b>	Show ONU description.

### 18.1.8 Configure ONU downstream encryption

When enable ONU downstream encryption, you should also enable PON downstream encryption at the same time. In another word, it's not effective if only enable ONU downstream encryption. By default, ONU downstream encryption is disabled.

Begin at privileged configuration mode, enable ONU downstream encryption as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon slot/port</b>	Enter PON interface configuration mode.
<b>Step 3</b>	<b>onu&lt;onuid&gt;encryption{enable disable}</b>	Enable/Disable ONU downstream encryption.
<b>Step 4</b>	<b>show onu&lt;onuid&gt;encryption</b>	Show onu downstream encryption.

### 18.1.9 Configure ONU upstream bandwidth

You can configure upstream bandwidth for authorized ONU. Begin at privileged configuration mode, configure ONU upstream bandwidth as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3a	<b>onu &lt;onuid&gt; upstream fir &lt;0-950000&gt; cir &lt;1-950000&gt; pir &lt;512-1000000&gt; weight &lt;1-20&gt;</b>	Configure ONU upstream bandwidth. When fir is 0, it means no fixed bandwidth. Fir, cir and pir should satisfy this condition: FIR<=CIR<=PIR.
Step 3b	<b>no onu &lt;onuid&gt; upstream</b>	Delete ONU upstream bandwidth configuration.
Step 4	<b>show onu &lt;onuid&gt; upstream</b>	Show onu upstream bandwidth.

#### 18.1.10 Configure ONU downstream bandwidth

You can configure downstream bandwidth for authorized ONU. Begin at privileged configuration mode, configure ONU downstream bandwidth as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3a	<b>onu &lt;onuid&gt; downstream pir &lt;0-1000000&gt; weight &lt;1-16&gt;</b>	Configure ONU downstream bandwidth.
Step 3b	<b>no onu &lt;onuid&gt; downstream</b>	Delete ONU downstream bandwidth configuration.
Step 4	<b>show onu &lt;onuid&gt; downstream</b>	Show onu downstream bandwidth.

#### 18.1.11 Configure ONU MAC limit

Limite the ONU MAC address

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3	<b>onu &lt;1-65535&gt;[mac-limit] &lt;0-16383&gt;</b>	Set the onu mac limit
Step 4	<b>Show onu &lt;1-65535&gt;[mac-limit]</b>	Show the MAC limit count

### 18.1.12 Show ONU status

Can show the time of onu register, deregister and running

	Command	Function
Step 1	<b>configure terminal</b>	Enter globalconfiguration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3	<b>show onustatus &lt;all&gt;</b>	Show ONU status

### 18.1.13 Show ONU statistics

Begin at privileged configuration mode, show ONU statistics as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter globalconfiguration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3	<b>show onu &lt; 1-65535 &gt; statistics</b>	Show ONU statistics.

## 18.2 ONU global configuration

### 18.2.1 Show ONU information

All ONU information can be showed in PON interface configuration mode. Input this command **interface epon *slot/port*** to enter PON interface mode.

Command	Function
<b>show onu &lt; <i>onuid</i> &gt; ctc onu_info</b>	Display ONU basic information.
<b>show onu &lt; <i>onuid</i> &gt; ctc ctc_info</b>	Display CTC OAM version which ONU supports.
<b>show onu &lt; <i>onuid</i> &gt; ctconu_sn</b>	Display ONU vendor ID, version and PON MAC.
<b>show onu &lt; <i>onuid</i> &gt; ctcfw_ver</b>	Display PON firmware version.
<b>show onu &lt; <i>onuid</i> &gt; ctc chip_id</b>	Display PON chipset model.
<b>show onu &lt; <i>onuid</i> &gt; ctc cap_1</b>	Display ONU main specifications; include port number, port type, upstream queue number, maximum upstream port queue number, downstream queue number, maximum

	downstream port queue number and backup battery.
<b>show onu</b> <onuid> <b>ctc opm_diag</b>	Display ONU optical transceiver main parameters and diagnosis.
<b>show onu</b> <onuid> <b>ctc cap_2</b>	Display ONU main specifications; include multi LLID, protection type, slot number, port type and number, backup battery.
<b>show onu</b> <onuid> <b>ctc cap_3</b>	Display ONU IPv6 capability and transceiver power force shutdown.
<b>show onu</b> <onuid> <b>ctc fast_leave_ability</b>	Display ONU multicast fast leave capability.
<b>show onu</b> <onuid> <b>ctc fec_ability</b>	Display ONU FEC capability.
<b>show onu</b> <onuid> <b>ctc power_saving_cap</b>	Display ONU energy-saving capability and wake up mechanism.

### 18.2.2 Update ONU image

Only authorized ONU can be updated by this way. Begin at privileged configuration mode, configure ONU LOID authentication mode as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>upgrade onu image</b> <filename> <A.B.C.D>	Configure ONU firmware name and TFTP server.
Step 3	<b>upgrade onu select pon</b> <pon_num> {<onuid_list>}*8	Select ONU. ONU ID format is 1-2.
Step 4	<b>upgrade onu start</b>	Download ONU firmware and save in memory, and then update ONU.

#### Notice:

1. DO NOT turn power off when updating. After finishing update, OLT will inform ONU if updated successfully and reset ONU with the new firmware.
2. After ONU updated and restarted, OLT will send commit command to confirm the new version.
3. Please delete the firmware and upgrade settings by command **upgrade onu stop**.
4. Display ONU upgrade progress by command **show upgrade onu status**.
5. Display ONU upgrade settings by command **show upgrade onu info**.
6. Stop upgrading ONU by command **upgrade onu stop**.

### 18.2.3 Auto upgrade ONU

Add the ONU upgrade list, system will check the match ONU, upgrade the match ONU automatic

.Only can create one list in the same time.

Command	Function
---------	----------

<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>auto-upgrade</b> <i>&lt;force&gt;</i> <i>&lt;onu&gt;</i> <b>vendor</b> <i>&lt;string&gt;</i> <b>model</b> <i>&lt;string&gt;</i> <b>swversion</b> <i>&lt;string&gt;</i> <b>image</b> <i>&lt;filename&gt;</i> <i>&lt;A.B.C.D&gt;</i>	Configure ONU firmware vendor id ,model id, swversion,file name and TFTP server.

**Notice:**

1. When the ONU come online, the OLT will upgrade the ONU automatically.
2. DO NOT turn power off when updating. After finishing update, OLT will inform ONU if updated successfully and reset ONU with the new firmware.
3. Display ONU upgrade progress by command **show upgrade onu status**.
5. Display ONU upgrade settings by command **show auto-upgradeinfo**.
6. Delete the auto upgrade list: **no auto-upgrade onu vendor***<string>***model***<string>*

**18.2.4 Configure ONU management IP**

Begin at privileged configuration mode, configure ONU management IP as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon</b> <i>slot/port</i>	Enter PON interface configuration mode.
<b>Step 3</b>	<b>onu</b> <i>&lt;onuid&gt;</i> <b>etc mgmt ip</b> <i>&lt;A.B.C.D&gt;</i> <b>mask</b> <i>&lt;A.B.C.D&gt;</i> <b>[gw</b> <i>&lt;A.B.C.D&gt;</i> <b>]*I</b> <b>[cvlan</b> <i>1-4095&gt;</i> <b>]*I</b> <b>[svlan</b> <i>&lt;1-4095&gt;</i> <b>]*I</b> <b>[pri</b> <i>&lt;0-7&gt;</i> <b>]*I</b>	Configure ONU management IP.
<b>Step 4</b>	<b>show onu</b> <i>&lt;onuid&gt;</i> <b>etc mgmt</b>	Show ONU management IP.

**18.2.5 Configure ONU SNMP**

Begin at privileged configuration mode, configure ONU SNMP parameters as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon</b> <i>slot/port</i>	Enter PON interface configuration mode.
<b>Step 3</b>	<b>onu</b> <i>&lt;onuid&gt;</i> <b>ctcmdu_snmp v2 host</b> <i>&lt;A.B.C.D&gt;</i> <b>trap-port</b> <i>&lt;1-65535&gt;</i> <b>snmp-port</b> <i>&lt;1-65535&gt;</i> <b>name</b> <i>&lt;string&gt;</i> <b>[com_rd</b> <i>&lt;string&gt;</i> <b>]*1</b> <b>[com_wr</b> <i>&lt;string&gt;</i> <b>]*1</b>	Configure MDU SNMP parameters.
<b>Step 4</b>	<b>show onu</b> <i>&lt;onuid&gt;</i> <b>etc md_u_snmp</b>	Show MDU SNMP

	configurations.
--	-----------------

### 18.2.6 Configure ONU multi LLID

Begin at privileged configuration mode, configure ONU multi LLID as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3	<b>onu&lt;onuid&gt; ctc multi_llid&lt;0-8&gt;</b>	Configure number of ONU LLID. 0: return to S-LLID mode. 1~8: number of LLID.

### 18.2.7 Configure ONU primary PON interface

Begin at privileged configuration mode, configure ONU primary PON interface as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3	<b>onu&lt;onuid&gt; ctc active_pon&lt;0-8&gt;</b>	Configure ONU primary PON interface.
Step 4	<b>show onu&lt;onuid&gt; ctc active_pon</b>	Show ONU primary PON interface.

### 18.2.8 Configure ONU FEC function

Begin at privileged configuration mode, configure ONU FEC function as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3	<b>onu &lt;onuid&gt; ctc fec_mode {enable disable}</b>	Enable/Disable ONU FEC function.
Step 4	<b>show onu&lt;onuid&gt; ctc fec_mode</b>	Show ONU FEC function configuration.

### 18.2.9 Configure optical link protection

In optical link protection system, ONU should hold register status in holdover time. Begin at privileged configuration mode, configure optical link protection as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3	<b>onu &lt;onuid&gt; ctc holdover &lt;0-65535&gt;</b>	Configure optical link protection. value 0 means protection is disabled.
Step 4	<b>show onu &lt;onuid&gt; ctc holdover</b>	Show onu optical link protection configuration.

### 18.2.10 Configure ONU SLA function

Begin at privileged configuration mode, configure ONU SLA function as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3	<b>onu &lt;onuid&gt; ctc sladisable</b>	Disable ONU SLA function.
Step 4a	<b>onu &lt;onuid&gt; ctc sla enable sp_basic</b>	Enable ONU SLA function.
Step 4b	<b>onu &lt;onuid&gt; ctc sla enable {wrr sp_wrr} {queue &lt;1-8&gt; fix_packet_size &lt;0-1900&gt; fix_bandwidth &lt;0-1024&gt; guaranteed_bandwidth &lt;1-1024&gt; best_effort_bandwidth &lt;1-1024&gt; weight &lt;0-100&gt;} *8</b>	Enable SLA function and configure weight of each queue.
Step 5	<b>show onu &lt;onuid&gt; ctc sla</b>	Show ONU SLA configurations.

### 18.2.11 Configure ONU multicast mode

Begin at privileged configuration mode, configure ONU multicast mode as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.

<b>Step 2</b>	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
<b>Step 3</b>	<b>onu <i>&lt;onuid&gt;</i> ctcmc_switch {snooping control}</b>	Snooping: enable IGMP/MLD Snooping protocol for multicast member management. Control: enable CTC controllable multicast protocol for member management.
<b>Step 4</b>	<b>show onu <i>&lt;onuid&gt;</i> ctc mc_switch</b>	Show ONU multicast mode configuration.

### 18.2.12 Configure ONU fast leave function

Begin at privileged configuration mode, configure ONU fast leave function as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
<b>Step 3</b>	<b>onu <i>&lt;onuid&gt;</i> ctc fast_leave {enable disable}</b>	Enable or disable ONU fast leave function.
<b>Step 4</b>	<b>show onu <i>&lt;onuid&gt;</i> ctc fast_leave</b>	Show onu fast leave configuration.

### 18.2.13 Restart ONU

Begin at privileged configuration mode, restart ONU as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
<b>Step 3</b>	<b>onu <i>&lt;onuid&gt;</i> ctc reset</b>	Restart ONU.

### 18.2.14 Configure ONU power saving mode

Begin at privileged configuration mode, configure ONU power saving mode as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter gloable configuration mode.
<b>Step 2</b>	<b>interface epon <i>slot/port</i></b>	Enter PON interface

		configuration mode.
<b>Step 3</b>	<b>onu</b> <1-65535> <b>ctc</b> <b>power_saving_cfg</b> early_wakeup[enable disable] <b>sleep_duration_max</b> <0-65535>	Enable: enable early wake up mechanism. Disable: disable early wake up mechanism. <0-65535>: maximum refresh time of power saving mechanism, unit is TQ.
<b>Step 4</b>	<b>show onu</b> <onuid> <b>ctc power_saving_cfg</b>	Show ONU power saving configurations.

### 18.2.15 Configure ONU sleep duration and wake up duration

Begin at privileged configuration mode, configure ONU sleep duration and wake up duration as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon</b> <i>slot/port</i>	Enter PON interface configuration mode.
<b>Step 3</b>	<b>onu</b> <onuid> <b>ctc</b> <b>sleep_ctrl</b> sleep_duration<0-65535> <b>wake_duration</b> <0-65535> <b>sleep_flag</b> [off on change] <b>sleep_mode</b> [none tx_sleep_only tx_and_rx_sleep]	<b>sleep_flag:Off</b> means ONU out of power saving status. <b>On</b> means ONU is in power saving status. <b>Change</b> means change ONU power saving mode, sleep duration and wake up duration. <b>sleep_mode:tx_sleep_only</b> means transmitter's sleep mode. <b>tx_and_rx_sleep</b> means transmitter and receiver's sleep mode.
<b>Step 4</b>	<b>show onu</b> <onuid> <b>ctc sleep_ctrl</b>	Show ONU power saving mode, sleep duration and wake up duration.

### 18.2.16 Configure ONU optical link protection mechanism

Begin at privileged configuration mode, configure ONU optical link protection mechanism as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon</b> <i>slot/port</i>	Enter PON interface

		configuration mode.
<b>Step 3</b>	<b>onu</b> <onuid> <b>ctc pon_protect</b> <b>los_optical</b> <0-65535> <b>los_mpcp</b> <0-65535>	<b>los_optical</b> :Confirmation time of invalid optical link by checking optical signal. Default value is 2 ms.  <b>los_mpcp</b> :Confirmation time of invalid optical link by checking MPCP messages. Default value is 55 ms.
<b>Step 4</b>	<b>show onu</b> <onuid> <b>ctcpon_protect</b>	Show optical link protection mechanism configurations.

### 18.2.17 Configure ONU PON power supply control

Begin at privileged configuration mode,configure ONU PON power supply control as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon</b> <i>slot/port</i>	Enter PON interface configuration mode.
<b>Step 3</b>	<b>onu</b> <onuid> <b>ctc laser action</b> <0-65535> <b>pon_mac</b> <xx.xx:xx.xx:xx.xx> <b>transmitter</b> [major standby both/]	Action: value 0 means turn on transmitter power again. Value 1-65534 means power supply turn-off time. Value 65535 means turn off power supply forever. Major:operation to current major optical module. Standby:operation to current standby optical module. Both:operation to major and standby optical module.

### 18.2.18 Configure ONU MAC aging time

Begin at privileged configuration mode,configure ONU MAC aging time as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon</b> <i>slot/port</i>	Enter PON interface configuration mode.

<b>Step 3</b>	<b>onu</b> <onuid> <b>ctc agetime</b> <0-65535>	Configure ONU MAC aging time. Value 0 means disable MAC aging. Value <1-65535> means MAC aging time. Unit: second.
---------------	---	--

### 18.2.19 Configure ONU PON port performance statistics

Configure ONU PON port performance statistics and period. Begin at privileged configuration mode, configure ONU PON port performance statistics as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon</b> <i>slot/port</i>	Enter PON interface configuration mode.
<b>Step 3</b>	<b>onu</b> <onuid> <b>ctc pon monitor_status</b> {enable disable}<0-65535>	Configure ONU PON port performance statistics and period. Period unit is second.
<b>Step 4</b>	<b>show onu</b> <onuid> <b>ctc pon monitor_status</b>	Show ONU PON port performance statistics configurations.

### 18.2.20 Clear/show ONU PON port statistics

Begin at privileged configuration mode, clear or show ONU PON port performance statistics as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon</b> <i>slot/port</i>	Enter PON interface configuration mode.
<b>Step 3</b>	<b>onu</b> <onuid> <b>ctc pon monitor_current</b>	Clear ONU PON port statistic.0
<b>Step 4a</b>	<b>show onu</b> <onuid> <b>ctc pon monitor_current</b>	Show ONU PON port current statistics.
<b>Step 4b</b>	<b>show onu</b> <onuid> <b>ctc pon monitor_histor0y</b>	Show ONU PON port previous period statistics.

## 18.3 ONU port configuration

### 18.3.1 Show onu port information

All ONU port information can be showed in PON interface configuration mode. Input this command **interface epon slot/port** to enter PON interface mode.

The information contains port type, link status, port administration status, flow control, speed, duplex and storm control. There may be some differences between different ONU.

<b>show onu</b> <onuid> <b>ctc eth</b> <port-num> <b>port_info</b>	Show ONU port information.
<b>show onu</b> <onuid> <b>ctc eth</b> <port-num> <b>linkstate</b>	Show ONU port link status.
<b>show onu</b> <onuid> <b>ctc eth</b> <port-num> <b>phy_info</b>	Show ONU port administration information.
<b>show onu</b> <onuid> <b>ctc eth</b> <port-num> <b>autoneg_local_cap</b>	Show ONU port AutoNeg Advertised Technology Ability.
<b>show onu</b> <onuid> <b>ctc eth</b> <port-num> <b>autoneg_adv_cap</b>	Show ONU port AutoNeg Local Technology Ability.

### 18.3.2 Enable/Disable ONU port

Begin at privileged configuration mode, enable or disable ONU port as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon slot/port</b>	Enter PON interface configuration mode.
Step 3	<b>onu</b> <onuid> <b>ctc eth</b> <port-num> <b>phy_ctrl</b> [enable disable]	Enable or disable ONU port.
Step 4	<b>show onu</b> <onuid> <b>ctc eth</b> <port-num> <b>phy_state</b>	Show ONU port administration state.

### 18.3.3 Configure ONU port autonegotiation

Begin at privileged configuration mode, configure ONU port autonegotiation as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon slot/port</b>	Enter PON interface configuration mode.
Step 3	<b>onu</b> <onuid> <b>ctc eth</b> <port-num> <b>autoneg</b> [enable disable]	Enable or disable ONU port autonegotiation.
Step 4	<b>show onu</b> <onuid> <b>ctc eth</b> <port-num> <b>autoneg</b>	Show ONU port autonegotiation state.

### 18.3.4 Configure ONU port re-autonegotiation

Begin at privileged configuration mode, configure ONU port re-autonegotiation as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3	<b>onu&lt;onuid&gt;ctc eth&lt;port-num&gt;autonegrestart</b>	Force ONU port restart negotiation.

### 18.3.5 Configure ONU port upstream policy

Begin at privileged configuration mode, configure ONU port upstream policy as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3	<b>onu&lt;onuid&gt;ctc eth&lt;port-num&gt;policy cir&lt;1-1048576&gt; [cbs] &lt;1-10240&gt; [ebs] &lt;1-10240&gt;</b>	Configure ONU port upstream policy.
Step 4	<b>onu&lt;onuid&gt;ctc eth&lt;port-num&gt;policy default</b>	Delete ONU port upstream policy.
Step 5	<b>show onu&lt;onuid&gt;ctc eth&lt;port-num&gt;policy</b>	Show ONU port upstream policy configuration.

### 18.3.6 Configure ONU port downstream rate limit

Begin at privileged configuration mode, configure ONU port downstream rate limit as the following table shows.

	command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3	<b>onu&lt;onuid&gt;ctc eth&lt;port-num&gt;rate_limit cir&lt;1-1048576&gt; [pir] &lt;1-1048576&gt;</b>	Configure ONU port downstream rate limit.
Step 4	<b>onu&lt;onuid&gt;ctc eth&lt;port-num&gt;rate_limit default</b>	Delete ONU port downstream rate limit.
Step 5	<b>show onu&lt;onuid&gt;ctc eth&lt;port-num&gt;rate_limit</b>	Show ONU port downstream policy configuration.

### 18.3.7 Configure ONU port flow control

Begin at privileged configuration mode, configure ONU port flow control as the following

table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3	<b>onu&lt;onuid&gt;ctc eth&lt;port-num&gt; flow_control[enable disable]</b>	Enable or disable ONU port flow control.
Step 4	<b>show onu&lt;onuid&gt;ctc eth&lt;port-num&gt;flow_control</b>	Show ONU port flow control configuration.

### 18.3.8 Configure ONU port loopback detection

Begin at privileged configuration mode, configure ONU port loopback detection as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3	<b>onu &lt;onuid&gt;ctc eth&lt;port-num&gt;loopdetect[enable disable]</b>	Enable or disable ONU port loopback detection.
Step 4	<b>showonu&lt;onuid&gt; ctc eth&lt;port-num&gt;loopdetect</b>	Show ONU port loopback detection configuration.

### 18.3.9 Configure ONU loop port auto-shutdown

When enabled this function, the port will shutdown if there is a loopback.

Begin at privileged configuration mode, configure ONU loop port auto-shutdown as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3	<b>onu&lt;onuid&gt;ctc eth&lt;port-num&gt;loop[enable disable]</b>	Enable: when it detects a loopback, the port will shutdown. Disable: when it detects a loopback, the port will not shutdown.

### 18.3.10 Configure ONU port VLAN mode.

There are five VLAN modes, transparent, tag, translation, trunk and aggregation.

Begin at privileged configuration mode, configure ONU port VLAN mode as the following table shows.

	<b>Command</b>	<b>function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
<b>Step 3</b>	<b>onu&lt;onuid&gt;etc eth&lt;port-num&gt;vlan mode [transparent tag translation aggregation trunk]</b>	Configure port VLAN mode.

### 18.3.11 Configure ONU port PVID

Only tag mode, translation mode, trunk mode and aggregation mode need to configure PVID.

Begin at privileged configuration mode, configure ONU port PVID as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
<b>Step 3</b>	<b>onu&lt;onuid&gt;etc eth&lt;port-num&gt;vlan pvid&lt;pvid&gt;pri&lt;pri&gt;</b>	Pvid range: 1-4095 Pri range: 0-7.

### 18.3.12 Configure ONU port VLAN translation entries

Begin at privileged configuration mode, configure ONU port VLAN translation entries as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
<b>Step 3</b>	<b>onu&lt;onuid&gt;etc eth&lt;port-num&gt;vlan translation[set add del] {&lt;old-vid&gt; to &lt;new-vid&gt;}*8</b>	Configure VLAN translation entries. old-vid: also called CVLAN. new-vid: also called SVLAN.

### 18.3.13 Configure ONU port VLAN trunk entries

Begin at privileged configuration mode, configure ONU port VLAN trunk entries as the following table shows.

<b>Command</b>	<b>Function</b>

<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon slot/port</b>	Enter PON interface configuration mode.
<b>Step 3</b>	<b>onu&lt;onuid&gt;ctc eth&lt;port-num&gt;vlantrunk[set add del] {&lt;vid&gt;}*8</b>	Configure VLAN trunk entries.

### 18.3.14 Configure ONU port VLAN aggregation entries

Begin at privileged configuration mode, configure ONU port VLAN aggregation entries as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon slot/port</b>	Enter PON interface configuration mode.
<b>Step 3</b>	<b>onu&lt;onuid&gt;ctc eth &lt;port-num&gt;vlan aggregationdst_vlan&lt;new-vid&gt;agg_vlan{&lt; old-vid&gt;}*8</b>	Configure VLAN aggregation entries. old-vid: also called CVLAN. new-vid: also called SVLAN.

### 18.3.15 Show ONU port VLAN configurations

Begin at privileged configuration mode, show ONU port VLAN configurations as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon slot/port</b>	Enter PON interface configuration mode.
<b>Step 3</b>	<b>show onu&lt;onuid&gt;ctc eth&lt;port-num&gt;vlan</b>	Show ONU port VLAN configurations.

### 18.3.16 Configure ONU port QoS function

QoS function includes data stream classification and mark. Customers can mark different streams by priority according to different rules.

This OLT supports these matchable conditions: VLAN ID, Ethernet type, priority, IP type, ToS, IP Precedence, layer 4 port, IP address, MAC address, and so on.

Begin at privileged configuration mode, configure ONU port QoS function as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global

		configuration mode.
<b>Step 2</b>	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
<b>Step 3 a</b>	<b>onu&lt;onuid&gt;ctc eth&lt;port-num&gt;class</b> <b>addprecedence&lt;1-8&gt;priority&lt;0-7&gt;</b> <b>[dst-mac{equal unequal}&lt;xx:xx:xx:xx:xx:xx&gt;]*1</b> <b>[src-mac {equal unequal}</b> <b>&lt;xx:xx:xx:xx:xx:xx&gt;]*1</b> <b>[vlan{equal unequal}&lt;1-4094&gt;]*1</b> <b>[cos{equal unequal}&lt;0-7&gt;]*1</b> <b>[ether-type {equal unequal}&lt;XXXX&gt;]*1</b> <b>[src-ip {equal unequal}&lt;A.B.C.D&gt;]*1</b> <b>[dest-ip {equal unequal}&lt;A.B.C.D&gt;]*1</b> <b>[protocol {equal unequal}&lt;0-255&gt;]*1</b> <b>[tos-dscp {equal unequal}&lt;0-255&gt;]*1</b> <b>[src-port {equal unequal}&lt;0-65535&gt;]*1</b> <b>[dest-port {equal unequal}&lt;0-65535&gt;]*1</b>	Configure port classification and mark rule.
<b>Step 3 b</b>	<b>onu&lt;onuid&gt;ctc eth&lt;port-num&gt;classdel</b> <b>precedence&lt;1-8&gt;</b>	Delete port classification and mark configurations.
<b>Step 3 c</b>	<b>onu&lt;onuid&gt;ctc eth&lt;port-num&gt;class clean</b>	Clear all port classification and mark configurations.
<b>Step 4</b>	<b>show onu&lt;onuid&gt; ctc eth&lt;port-num&gt;class</b>	Show port classification and mark configurations.

### 18.3.17 Configure ONU port multicast VLAN

Begin at privileged configuration mode, configure ONU port multicast VLAN as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
<b>Step 3a</b>	<b>onu &lt;onuid&gt; ctc eth &lt;port-num&gt;mc_vlan</b> <b>{add del} {&lt;1-4095&gt;}*8</b>	Add or delete port multicast VLAN.
<b>Step 3b</b>	<b>onu &lt;onuid&gt; ctc eth &lt;port-num&gt;mc_vlan</b> <b>clean</b>	Clear port multicast VLAN.
<b>Step 4</b>	<b>show onu &lt;onuid&gt; ctc eth &lt;port-num&gt;</b> <b>mc_vlan</b>	Show port multicast VLAN configurations.

### 18.3.18 Configure ONU port maximum multicast groups

Begin at privileged configuration mode, configure ONU port maximum multicast groups as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3	<b>onu</b> <onuid> <b>ctc eth</b> <port-num> <b>mc_maxgrp</b> <0-4096>	Configure ONU maximum multicast groups.
Step 4	<b>showonu</b> <onuid> <b>ctc eth</b> <port-num> <b>mc_maxgrp</b>	Show ONU maximum multicast groups.

### 18.3.19 Configure ONU port multicast VLAN strip

Begin at privileged configuration mode, configure ONU port multicast VLAN strip as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3a	<b>onu</b> <onuid> <b>ctc eth</b> <port-num> <b>mc_tagstrip {enable disable}</b>	Enable: strip VLAN tag of multicast streams and query message. Disable: don't strip VLAN tag of multicast streams and query message.
Step 3b	<b>onu</b> <onuid> <b>ctc eth</b> <port-num> <b>mc_tagstrip iptv set</b> {<1-4095> <b>to</b> <1-4095>}*8	Modify multicast customer VLAN and query message VLAN to IPTV VLAN.
Step 4	<b>show onu</b> <onuid> <b>ctc eth</b> <port-num> <b>mc_tagstrip</b>	Show ONU port multicast VLAN strip configurations.

### 18.3.20 Configure ONU port statistics

Begin at privileged configuration mode, configure ONU port data packets performance statistics as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter PON interface configuration mode.
Step 3	<b>onu</b> <1-65535> <b>ctc</b> <b>eth</b> <port-num> <b>monitor_status</b> <b>[enable disable]</b> <0-65535>	Configure performance statistics. Value <0-65535> is statistics

		period. Unit is second.
<b>Step 4</b>	<b>show onu</b> <onuid> <b>ctc</b> <b>eth</b> <port-num> <b>monitor_status</b>	Show ONU port performance statistics state and period.

### 18.3.21 Clear/Show ONU port statistics

Begin at privileged configuration mode, clear or show ONU port statistics as the following table shows.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon</b> <i>slot/port</i>	Enter PON interface configuration mode.
<b>Step 3</b>	<b>onu</b> <1-65535> <b>ctc</b> <b>eth</b> <port-num> <b>monitor_current</b>	Clear ONU port statistics.
<b>Step 4</b>	<b>show onu</b> <onuid> <b>ctc</b> <b>eth</b> <port-num> <b>monitor_current</b>	Show ONU port current period statistics.
<b>Step 5</b>	<b>show onu</b> <onuid> <b>ctc</b> <b>eth</b> <port-num> <b>monitor_history</b>	Show ONU port previous period statistics.

## 18.4 ONU remote voice configuration

### 18.4.1 Show basic information

All the onu voice information query are in this node: **interface epon** *slot/port*

Show the current voice module support voice protocol and number of the POTS, etc.

<b>show onu</b> <onuid> <b>ctc iad_info</b>	Show the current voice module support voice protocol and ,number of the POTS
<b>show onu</b> <onuid> <b>ctciad_status</b>	Show running state of IAD in H. 248 protocol
<b>show onu</b> <onuid> <b>ctcpots</b> <1-255> <b>pots_status</b>	Show the state of POTS

### 18.4.2 Configure global parameters

These commands are used to configure network of VoIP voice. This is must configure parameters.

	<b>Command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface epon</b> <i>slot/port</i>	Enter the pon interface configuration mode.
<b>Step 3a</b>	<b>onu</b> <onuid> <b>ctc</b>	Configure voice IP

	<b>voip_global_paramip_mode static ipaddr</b> <A.B.C.D> <b>netmask</b> <A.B.C.D> <b>gateway</b> <A.B.C.D>	addressmode is static
Step 3b	<b>onu</b> <onuid> <b>ctc</b> <b>voip_global_paramip_mode dhcp</b>	Configure voice IP address mode is DHCP
Step 3c	<b>onu</b> <onuid> <b>ctc</b> <b>voip_global_paramip_mode pppoe mode</b> {auto chap pap} <b>username</b> <string> <b>password</b> <string>	Configure voice IP address mode is PPPOE
Step 4	<b>onu</b> <onuid> <b>ctc</b> <b>voip_global_param</b> <b>vlan_mode</b> {transparent tag vlan_stacking} <b>cvlan</b> <0-4095> <b>svlan</b> <0-4095> <b>priority</b> <0-7>	Configure voice VLAN mode, if only cvlan, set the svlan is 0
Step 5	<b>show onu</b> <onuid> <b>ctc</b> <b>voip_global_param</b>	Show onu VoIP global parameters

### 18.4.3 Enable/disable POTS port

These commands are used to enable or disable POTS port.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon slot/port</b>	Enter PON interface configuration mode.
Step 3	<b>onu</b> <onuid> <b>ctc</b> <b>pots</b> <1-255> <b>port_manage</b> {enable disable}	Enable or disable POTS port.
Step 4	<b>show onu</b> <onuid> <b>ctc</b> <b>pots</b> <1-255> <b>port_manage</b>	Show POTS port administration status.

### 18.4.4 Configure H.248 protocol

These commands are used to configure parameters of H.248 protocol. This is must configure parameters

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon slot/port</b>	Enter the pon interface configuration mode.
Step 3a	<b>onu</b> <onuid> <b>ctc</b> <b>h248_param_configreg_mode ip_addr</b>	Configure H. 248 registration mode is IP.
Step 3b	<b>onu</b> <onuid> <b>ctc</b> <b>h248_param_configreg_mode</b> {realm_name device_name} <b>mid</b> <string>	Configure H. 248 registration mode is realm.
Step 4	<b>onu</b> <onuid> <b>ctc</b>	Configure onu heartbeat

	<b>h248_param_config</b> heartbeat <b>mode</b> {disable h248} <b>cycle</b> <1-65535> <b>count</b> <1-65535>	parameters.
Step 5	<b>onu</b> <onuid> <b>etc h248_param_config</b> <b>mg_port</b> <1-65535> <b>mgc_ip</b> <A.B.C.D> <b>mgc_port</b> <1-65535> [ <b>bak_mgc_ip</b> <A.B.C.D> <b>bak_mgc_port</b> <1-65535>]*1	Configure MGC and back up MGC informations.
Step 6	<b>show onu</b> <onuid> <b>etc h248_param_config</b>	Show onu VoIP parameters of H.248

#### 18.4.5 Configure POTS UserTID information(H.248)

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon</b> slot/port	Enter the pon interface configuration mode.
Step 3	<b>onu</b> <onuid> <b>ctcpots</b> <1-255> <b>h248_user_tid</b> <name>	Configure POTS UserTID information
Step 4	<b>show onu</b> <onuid> <b>etc pots</b> <1-255> <b>h248_user_tid</b>	Show POTS UserTID information

#### 18.4.6 Configure RTP TID information(H.248)

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon</b> slot/port	Enter the pon interface configuration mode.
Step 3	<b>onu</b> <onuid> <b>etc h248_rtp_tid</b> number <0-255> <b>prefix</b> <string> <b>digit_begin</b> <0-4294967295> <0-4294967295> <b>mode</b> {align unaligned} <b>digit_length</b> <0-255>	Configure RTP TID parameters
Step 4	<b>show onu</b> <onuid> <b>etc h248_rtp_tid</b>	RTP TID parameters

#### 18.4.7 Configure SIP protocol

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon</b> slot/port	Enter the pon interface configuration mode.
Step 3	<b>onu</b> <onuid>	Configure onu heartbeat

	<b>ctcsip_param_config</b> heartbeat <b>switch</b> {enable disable} <b>cycle</b> <1-65535> <b>count</b> <1-65535> {reg_interval <0-65535>}*1	parameters
Step 4	<b>onu</b> <onuid> <b>ctcsip_param_config</b> <b>mg_port</b> <1-65535> <b>out_bound_serv</b> <b>ip</b> <A.B.C.D> <b>port</b> <1-65535>	Configure MG port and outbound server IP address and port
Step 5	<b>onu</b> <onuid> <b>ctcsip_param_config</b> proxy_serv <b>ip</b> <A.B.C.D> <b>port</b> <1-65535>[ <b>bak_ip</b> <A.B.C.D> <b>bak_port</b> <1-65535>]*1	Configure proxy server or back up proxy server IP address and port,
Step 6	<b>onu</b> <onuid> <b>ctcsip_param_config</b> reg_serv <b>ip</b> <A.B.C.D> <b>port</b> <1-65535>[ <b>bak_ip</b> <A.B.C.D> <b>bak_port</b> <1-65535>]*1	Configure MG port and outbound server IP address and port
Step 7	<b>show onu</b> <onuid> <b>ctcsip_param_config</b>	Show ONU sip parameters

#### 18.4.8 Configure SIP account parameters of POTS

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon</b> <i>slot/port</i>	Enter the pon interface configuration mode.
Step 3	<b>onu</b> <onuid> <b>ctcpots</b> <1-255> <b>sip_user_config</b> <b>account</b> <account> <b>name</b> <name> <b>pwd</b> <password>	Configure SIP user information of POTS port
Step 4	<b>show onu</b> <onuid> <b>ctc</b> <b>pots</b> <1-255> <b>sip_user_config</b>	Show SIP user information

#### 18.4.9 Configure fax mode

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon</b> <i>slot/port</i>	Enter the pon interface configuration mode.
Step 3	<b>onu</b> <onuid> <b>ctcfax_modem_config</b> voice_t38 {enable disable} <b>control</b> {negotiation auto_vbd}	Configure fax mode and the way of negotiation

Step 4	<b>show onu &lt;onuid&gt; ctc fax_modem_config</b>	Show faxservice parameter information
--------	--	---------------------------------------

#### 18.4.10 VoIP module operation

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon slot/port</b>	Enter the pon interface configuration mode.
Step 3	<b>onu &lt;onuid&gt; ctc iad_oper {reregister deregister reset}</b>	Reregister: onu re-registration Deregister: onu logout Reset: reset VoIP module

#### 18.4.11 Configure SIP digitmap

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon slot/port</b>	Enter the pon interface configuration mode.
Step 3	<b>onu &lt;onuid&gt; ctc sip_digit_map num &lt;0-255&gt;&lt;0-255&gt;&lt;mapstr&gt;</b>	Configure SIP digitmap

### 18.5 ONU remote alarm information

All onu alarm used this template configuration,

#### 18.5.1 Showonu alarm information

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon slot/port</b>	Enter the pon interface configuration mode.
Step 3	<b>show onu &lt;onuid&gt; ctc alarm_cfg onu {equipment_alarm power_alarm battery_missing battery_failure battery_volt_low physical_intrusion onu_self_test_failure onu_temp_high_alarm onu_temp_low_alarm iad_connection_failure pon_if_switch sleep_status_update}</b>	Show ONU alarm status.
Step 4	<b>show onu &lt;onuid&gt; ctc alarm_thr onu {battery_volt_low onu_temp_high_alarm </b>	Show ONU alarm threshold.

<code>onu_temp_low_alarm}</code>
----------------------------------

### 18.5.2 Show onu pon alarm information

	Command	Function
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>interface epon slot/port</code>	Enter the pon interface configuration mode.
Step 3	<code>showonu&lt;onuid&gt;ctc {alarm_cfg alarm_thr} pon {rx_power_high_alarm rx_power_low_alarm tx_power_high_alarm tx_power_low_alarm tx_bias_high_alarm tx_bias_low_alarm vcc_high_alarm vcc_low_alarm temp_high_alarm temp_low_alarm rx_power_high_warning rx_power_low_warning tx_power_high_warning tx_power_low_warning tx_bias_high_warning tx_bias_low_warning vcc_high_warning vcc_low_warning temp_high_warning temp_low_warning}</code>	Show pon optical power, temperature, voltage, current alarm status and threshold alarm_cfg:onu alarm status alarm_thr:onu alarm threshold
Step 4	<code>show onu &lt;onuid&gt; ctc {alarm_cfg alarm_thr} pon {downstream_drop_events_alarm upstream_drop_events_alarm downstream_crcerror_frames_alarm upstream_crcerror_frames_alarm downstream_undersize_frames_alarm upstream_undersize_frames_alarm downstream_oversize_frames_alarm upstream_oversize_frames_alarm downstream_fragments_alarm upstream_fragments_alarm downstream_jabbers_alarm upstream_jabbers_alarm downstream_discards_alarm upstream_discards_alarm downstream_errors_alarm upstream_errors_alarm downstream_drop_events_warning upstream_drop_events_warning downstream_crcerror_frames_warning upstream_crcerror_frames_warning downstream_undersize_frames_warning upstream_undersize_frames_warning downstream_oversize_frames_warning upstream_oversize_frames_warning downstream_fragments_warning upstream_fragments_warning}</code>	Show the pon port statistical alarm status and threshold alarm_cfg:onu alarm status alarm_thr:onu alarm threshold

```
downstream_jabbers_warning|upstream_
jabbers_warning|downstream_discards_w
arning|upstream_discards_warning|down
stream_errors_warning|upstream_errors_
warning}
```

### 18.5.3 Show onu port alarm information

	Command	Function
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>interface epon <i>slot/port</i></code>	Enter the pon interface configuration mode.
Step 3	<code>show onu &lt;onuid&gt;etc alarm_cfg eth&lt;1-255&gt;{eth_port_auto_neg_failure eth_port_lo eth_port_failure eth_port_loopback eth_port_congestion}</code>	Query port alarm status alarm_cfg:onu alarm status
Step 4	<code>show onu&lt;onuid&gt;etc{alarm_cfg alarm_thr}eth&lt;1-255&gt;{downstream_drop_events_alarm upstream_drop_events_alarm downstream_crcerror_frames_alarm upstream_crcerror_frames_alarm downstream_undersize_frames_alarm upstream_undersize_frames_alarm downstream_oversize_frames_alarm upstream_oversize_frames_alarm downstream_fragments_alarm upstream_fragments_alarm downstream_jabbers_alarm upstream_jabbers_alarm downstream_discards_alarm upstream_discards_alarm downstream_errors_alarm upstream_errors_alarm status_change_times_alarm downstream_drop_events_warning upstream_drop_events_warning downstream_crcerror_frames_warning upstream_crcerror_frames_warning downstream_undersize_frames_warning upstream_undersize_frames_warning downstream_oversize_frames_warning upstream_oversize_frames_warning}</code>	Show the LAN port statistical alarm status and threshold  alarm_cfg:onu alarm status alarm_thr:onu alarm threshold

downstream_fragments_warning upstream_fragments_warning  downstream_jabbers_warning upstream_jabbers_warning  downstream_discards_warning upstream_discards_warning  downstream_errors_warning upstream_errors_warning  status_change_times_warning}	
--	--

#### 18.5.4 Show onupots alarm information

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter the pon interface configuration mode.
Step 3	<b>show onu &lt;1-65535&gt; ctc alarm_cfg pots &lt;1-64&gt; pots_port_failure</b>	Show pots alarm status

#### 18.5.5 Showonu E1 alarm information

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter the pon interface configuration mode.
Step 3	<b>show onu &lt;onuid&gt;ctc alarm_cfg e1 &lt;1-16&gt;[e1_port_failure e1_timing_unlock  e1_los]</b>	Show E1 alarm status

### 18.6 ONU remote private oam configuration

#### 18.6.1 Show ONU version of software|hardware

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter the pon interface configuration mode.
Step 3	<b>show onu &lt;onuid&gt;pri onu_ver</b>	Show ONU version of software hardware

**18.6.2 Show ONU light and port status**

	<b>Command</b>	<b>Function</b>
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter the pon interface configuration mode.
Step 3	<b>show onu &lt;onuid&gt; pri onu_status</b>	Show onu light and port status

**18.6.3 Configure MAC address aging time**

	<b>Command</b>	<b>Function</b>
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter the pon interface configuration mode.
Step 3	<b>onu &lt;onuid&gt; pri age_time &lt;0-630&gt;</b>	Configure the MAC address aging time
Step 4	<b>show onu &lt;onuid&gt; ctc pri age_time</b>	Show the MAC address aging time

**18.6.4 Port maxMAC addresses**

	<b>Command</b>	<b>Function</b>
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter the pon interface configuration mode.
Step 3	<b>onu &lt;onuid&gt; pri eth &lt;1-255&gt; mac_limit &lt;0-65535&gt;</b>	Limit the port number of MAC addresses learning
Step 4	<b>show onu &lt;onuid&gt; pri eth &lt;1-255&gt; mac_limit</b>	Show the port number of MAC addresses learning

**18.6.5 Show port MAC address table**

	<b>Command</b>	<b>Function</b>
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter the pon interface configuration mode.
Step 3	<b>show onu &lt;onuid&gt; pri</b>	Show port MAC address table

<b>eth&lt;1-255&gt;port_mac</b>	
---------------------------------	--

### 18.6.6 Port isolate enable|disable

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon slot/port</b>	Enter the pon interface configuration mode.
Step 3	<b>onu&lt;onuid&gt;pri port_isolate [enable disable]</b>	Configure the port isolate enable disable
Step 4	<b>show onu &lt;onuid&gt;pri port_isolate</b>	Show the status of pore isolate

### 18.6.7 Configure port negotiation mode

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon slot/port</b>	Enter the pon interface configuration mode.
Step 3	<b>onu &lt;onuid&gt;pri eth &lt;1-255&gt;mode_control[10hd 10fd 100hd 100fd 1000hd 1000fd 10000fd]</b>	Configure port negotiation mode
Step 4	<b>show onu &lt;onuid&gt;pri eth &lt;1-255&gt;mode_control</b>	Show the port configuration negotiation mode

### 18.6.8 Show the port actually negotiation mode

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon slot/port</b>	Enter the pon interface configuration mode.
Step 4	<b>show onu &lt;onuid&gt;pri eth &lt;1-255&gt;mode_status</b>	Show the port actually negotiation mode

### 18.6.9 Show port statistics

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon slot/port</b>	Enter the pon interface

		configuration mode.
Step 3	<b>show onu &lt;onuid&gt; pri eth &lt;1-255&gt; ethernet_stat</b>	Show the port statistics of data packet

### 18.6.10 Configure port storm-control

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon slot/port</b>	Enter the pon interface configuration mode.
Step 3	<b>onu &lt;onuid&gt; pri eth &lt;1-255&gt; pkg_suppress broddcast &lt;0-1024000&gt; multicast &lt;0-1024000&gt; unknown &lt;0-1024000&gt;</b>	Configure port broadcast, multicast and unicast unknown storm suppression
Step 4	<b>show onu &lt;onuid&gt; pri eth &lt;1-255&gt; pkg_suppress</b>	Show lan port storm suppression

### 18.6.11 WiFi configuration

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon slot/port</b>	Enter the pon interface configuration mode.
Step 3a	<b>onu &lt;onuid&gt; pri wifi_switch disable</b>	disable WiFi
Step 3b	<b>onu &lt;onuid&gt; pri wifi_switch enable {FCC ETSI} &lt;0-1&gt; {80211b 80211g 80211bg 80211n 80211bn} &lt;0-20&gt;</b>	Enable WiFi ETSI:European standard FCC:American standard <0-1>: 0 means automatically choose the channel number <0-20 > : transmission power, 0 to 20 DBM
Step 4	<b>Show onu &lt;onuid&gt; pri wifi_switch</b>	

### 18.6.12 SSID basic configuration

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon slot/port</b>	Enter the pon interface configuration mode.
Step 3a	<b>onu &lt;onuid&gt; pri {wifi_ssid0 wifi_ssid1 wifi_ssid2 wifi_ssid3}</b>	Enable / disable SSID

	<b>}</b> {enable/disable}	
Step 3b	<b>onu</b> <onuid> <b>pri</b> {wifi_ssid0 wifi_ssid1 wifi_ssid2 wifi_ssid3 } <b>name</b> <string> <b>hide</b> {enable/disable}auth_mode {open shared wepauto wpapsk wpa wpa2p sk wpa2 wpa/wpa2 wpapsk/wpa2psk waip sk wai} <b>encrypt_type</b> {none wep tkip aes tkipaes wpi}	Name string: ssid string hide [enable/disable],enable:hide,disa ble: Don't hide auth_mode:WLAN authentication mode encrypt_type:WLAN encryption type
Step 3c	<b>onu</b> <onuid> <b>pri</b> {wifi_ssid0 wifi_ssid1 wifi_ssid2 wifi_ssid3 } <b>wpa shared_key</b> <string> <b>rekey_interval</b> <0-4194303>	Shared_key: WPA Shared key, when authentication mode for WPAPSK or WPA2PSK, this configuration is effective. Rekey_interval: WPA key update interval
Step 3d	<b>onu</b> <onuid> <b>pri</b> {wifi_ssid0 wifi_ssid1 wifi_ssid2 wifi_ssid3 } <b>radius serverip type</b> {ipv4 ipv6 ipv4z ipv6z dns}len <1-255> <b>ip</b> <string> <b>prefixlen</b> <0-255> <b>port</b> <0-65535> <b>key</b> <string>	Type: Type of the RADIUS server IP address Len: the RADIUS server IP address length, authentication for WPA, connected, WPA/connected effectively Ip: the RADIUS server Ip address, authentication for WPA, connected, WPA/connected effectively Prefixlen: the RADIUS server address prefix length Port: the RADIUS server Port Key: the RADIUS server password
Step 3e	<b>onu</b> <onuid> <b>pri</b> {wifi_ssid0 wifi_ssid1 wifi_ssid2 wifi_ssid3 } <b>wep encryptionlevel</b> {40 104} <b>keyindex</b> <1-4> <b>key1</b> <string> <b>key2</b> <string> <b>key3</b> <string> <b>key4</b> <string>	Encryptionlevel: WEP key length Keyindex: key index, when encryption mode to WEP, this field is valid. key1-4:WEP keys 1-4
Step 3f	<b>onu</b> <onuid> <b>pri</b> {wifi_ssid0 wifi_ssid1 wifi_ssid2 wifi_ssid3 } <b>wapi type</b> {ipv4 ipv6} <b>serverip</b> <ipstring> <b>port</b> <1-65535>	Type:Type of wapi Serverip:wapi ip address Port:wapi port
Step 3g	<b>onu</b> <onuid> <b>pri</b> {wifi_ssid0 wifi_ssid1 wifi_ssid2 wifi_ssid3 } <b>commit</b>	Submit all configuration

Step 4	<b>show onu &lt;onuid&gt; pri {wifi_ssid0 wifi_ssid1 wifi_ssid2 wifi_ssid3}</b>	show ssid configuration
--------	---	-------------------------

### 18.6.13 Configure WAN connection

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon slot/port</b>	Enter the pon interface configuration mode.
Step 3a	<b>onu &lt;1-65535&gt; pri wan_conn index &lt;1-8&gt; delete</b>	Delete WAN connection
Step 3b	<b>onu &lt;1-65535&gt; pri wan_conn add bridge [internet other]</b>	Add bridge mode connection
Step 3c	<b>onu &lt;1-65535&gt; pri wan_conn add route [internet multicast tr069 tr069_internet tr069_voip voip_internet tr069_voip_internet other] {nat [enable disable]}*1</b>	Add route mode connection
Step 3d	<b>onu &lt;1-65535&gt; pri wan_conn index &lt;1-8&gt; bridge [internet other]</b>	Configure bridge mode connection
Step 3e	<b>onu &lt;1-65535&gt; pri wan_conn index &lt;1-8&gt; route [internet multicast tr069 tr069_internet tr069_voip voip_internet tr069_voip_internet other] {nat [enable disable]}*1</b>	Configure route mode connection
Step 3f	<b>onu &lt;1-65535&gt; pri wan_conn index &lt;1-8&gt; dhcp</b>	Configure WAN connection way to obtain the address is DHCP mode
Step 3g	<b>onu &lt;1-65535&gt; pri wan_conn index &lt;1-8&gt; static ip &lt;A.B.C.D&gt; mask &lt;A.B.C.D&gt; gw &lt;A.B.C.D&gt; dns master &lt;A.B.C.D&gt; slave &lt;A.B.C.D&gt;</b>	Configure WAN connection way to obtain the address is static mode
Step 3h	<b>onu &lt;1-65535&gt; pri wan_conn index &lt;1-8&gt; pppoe proxy [enable disable] user &lt;name&gt; pwd &lt;password&gt; server &lt;name&gt; mode [auto payload]</b>	Configure WAN connection way to obtain the address is PPPoE mode
Step 3i	<b>onu &lt;1-65535&gt; pri wan_conn index &lt;1-8&gt; vlan [tag transparent] &lt;1-4085&gt; {&lt;0-7&gt;}*1</b>	Configure vlan mode
Step 3j	<b>onu &lt;1-65535&gt; pri wan_conn index &lt;1-8&gt; translation vlan &lt;1-4085&gt; {&lt;0-7&gt;}*1</b>	Configure VLAN translation
Step 3k	<b>onu &lt;1-65535&gt; pri wan_conn index</b>	Configure VLAN QinQ

	<code>&lt;1-8&gt;qinq tpid &lt;1-65534&gt; vlan &lt;1-4085&gt; {[cos] &lt;0-7&gt;}*1</code>	
Step 3l	<code>onu &lt;1-65535&gt; pri wan_conn index &lt;1-8&gt; [vlan translation qinq] disable</code>	Disable vlan/translation/ qinq function
Step 3m	<code>onu &lt;1-65535&gt; pri wan_conn commit</code>	Submit wan connection configuration
Step 4	<code>Show onu &lt;1-65535&gt; pri wifi_switch</code>	Show wan connection configuration

#### 18.6.14 Configure IGMP enable/disable

	Command	Function
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>interface epon slot/port</code>	Enter the pon interface configuration mode.
Step 3	<code>onu&lt;onuid&gt;pri igmp_admin[enable disable]</code>	Configure IGMP enable/disable
Step 4	<code>show onu &lt;onuid&gt;pri igmp_admin</code>	Show IGMP status

#### 18.6.15 Configure CATV management

	Command	Function
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>interface epon slot/port</code>	Enter the pon interface configuration mode.
Step 3	<code>onu&lt;onuid&gt;pri catv_status[enable disable]</code>	Configure CATV management
Step 4	<code>show onu &lt;onuid&gt;pri catv_status</code>	Show the CATV management status

#### 18.6.16 Configure CTC OAM ignore

	Command	Function
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>interface epon slot/port</code>	Enter the pon interface configuration mode.
Step 3	<code>onu&lt;onuid&gt;pri ctcoam_skip[enable disable]</code>	Configure CTC OAM ignore
Step 4	<code>show onu &lt;onuid&gt;pri ctcoam_skip</code>	Show CTC OAM ignore status

#### 18.6.17 Configure reset to default

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter the pon interface configuration mode.
Step 3	<b>onu&lt;onuid&gt;pri factory_reset</b>	Reset to default

#### 18.6.18 Configure clean the MAC table

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter the pon interface configuration mode.
Step 3	<b>onu&lt;onuid&gt;pri mac_clean</b>	Configure clean the MAC table

#### 18.6.19 Save the ONU configuration

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter the pon interface configuration mode.
Step 3	<b>onu&lt;onuid&gt;pri save_config</b>	Save the ONU configuration

### 18.7 Show/Remove onu configuration

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon <i>slot/port</i></b>	Enter the pon interface configuration mode.
Step 3	<b>show onu running-config</b>	Show the onu running configuration of this PON port

Use the “no” command to remove the corresponding configuration. But it will take effect next time the ONU registered. When ONU has bound a template and the settings you will remove exist in it, the template will take effect.

Begin at privileged configuration mode, remove ONU configurations as the following table shows.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface epon slot/port</b>	Enter PON interface configuration mode.
Step 3a	<b>no onu &lt;onuid&gt; {upstream downstream}</b>	Remove ONU upstream or downstream bandwidth configuration.
Step 3b	<b>no onu &lt;onuid&gt; ctc {sla holdover mgmt mdu_snmp active_pon mc_switch fast_leave fec_mode voip_global_param h248_param_config h248_rtp_tid sip_param_config fax_modem_config sip_digit_map power_saving_cfg pon_protect agetime multi_llid sleep_ctrl}</b>	Remove ONU global configurations.
Step 3c	<b>no onu &lt;onuid&gt; ctc eth {&lt;1-255&gt; all} {flow_control policy rate_limit loopdetect disableloop monitor_status monitor_current vlan class mc_vlan mc_tagstrip mc_maxgrp phy_ctrl autoneg pvid}</b>	Remove ONU LAN configuration.
Step 3d	<b>no onu &lt;onuid&gt; ctc pots {&lt;1-255&gt; all} {h248_user_tid sip_user_config port_manage}</b>	Remove ONU POTS configurations.
Step 3e	<b>no onu &lt;onuid&gt; pri {age_time wifi_switch wifi_ssid0 wifi_ssid1 wifi_ssid2 wifi_ssid3 wan_conn}</b>	Remove ONU private OAM configured parameters.
Step 3f	<b>no onu &lt;onuid&gt; pri eth &lt;1-255&gt; {pkg_suppress mac_limit}</b>	Remove ONU private OAM configured LAN parameters.

## 18.8 ONU template management

### 18.8.1 Summary of the ONU template

Template under “config” node, the operation steps are as follows:

1. Create a template  
profile [dba|srv|voip|alarm] add {<1-32767>}\*1
2. Through profile\_id into the corresponding template node  
profile [dba|srv|voip|alarm] id <1-32767>
3. Modify the template parameters  
modify...

4. Exit template node  
exit
5. Binding template to an onu equipment  
Interface epon slot/port  
onu <1-65535> profile [dba|srv|voip|alarm] id <0-32767>
6. Query onu equipment binding template  
Interface epon slot/port  
Show onu <1-65535> profile\_id
7. query template configuration information  
show profile [dba|srv|voip|alarm]id <1-32767>  
query template binding the onu  
show profile [dba|srv|voip|alarm]id <1-32767> bind

### 18.8.2 DBA bandwidth template configuration

The default system will have an id 0 dba template, this template parameters cannot be modified, all onu when create the default binding in the template. Each ONU must bind a dba template.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>profile dbaadd</b> {<1-32767>}*1	Create a DBA template
Step 3	<b>profile dbaid</b> <1-32767>	Enter the DBA template node
Step 4	<b>modify</b> <b>fir</b> <0-950000> <b>cir</b> <1-950000> <b>pir</b> <512-1000000> <b>weight</b> <1-20>	When fir value is 0, said can not fixed bandwidth; Otherwise the three parameters to satisfy the following conditions: FIR<=CIR<=PIR.
Step 5	<b>commit</b>	Commit the template configuration
Step 6	<b>exit</b>	Exit template node
Step 7	<b>interface epon</b> slot/port	Enter the pon interface configuration mode.
Step 8	<b>onu</b> <onuid> <b>profile dba id</b> <1-32767>	Binding the dba template to set corresponding onu
Step 9	<b>show onu</b> <onuid> <b>profile_id</b>	Query the onu binding template accordingly
Step 10	<b>exit</b>	Exit the pon interface node
Step 11	<b>show profile dba id</b> <0-32767>	Show template configuration
Step 12	<b>show profile dba id</b> <0-32767> <b>bind</b>	Show onu bindings in the template
Step 13	<b>no profile dba id</b> <1-32767>	Delete the dba template

### 18.8.3 Services(SRV) template configuration

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>profile srv add</b> {<1-32767>}*1	Create the SRV template
Step 3	<b>profile srv id</b> <1-32767>	Enter the SRV template node
Step 4	<b>modify lan_count</b> <0-255>	Configure lan port quantity of template
Step 5	<b>commit</b>	Commit the template configuration
Step 6	<b>exit</b>	Exit template node
Step 7	<b>interface epon</b> slot/port	Enter the pon interface configuration mode.
Step 8	<b>onu</b> <onuid> <b>profile srv id</b> <1-32767>	Binding the SRV template to set correspondin
Step 9	<b>show onu</b> <onuid> <b>profile_id</b>	Query the onu binding template accordingly
Step 10	<b>exit</b>	Exit the pon interface node
Step 11	<b>show profile srv id</b> <0-32767>	Show template configuration
Step 12	<b>show profile srv id</b> <0-32767> <b>bind</b>	Show onu bindings in the template
Step 13	<b>no profile srv id</b> <1-32767>	Delete the srv template

The SRV template has the following configuration:

#### 1.Lan port number(s)

modify [lan\_count] <0-255>

#### 2.Multicast fast leave

modify c fast\_leave [enable|disable]

#### 3.FEC

modify c fec\_mode [enable|disable]

#### 4.Multicast mode

modify c [mc\_switch] [snooping|control]

#### 5.Onu llid number(s)

modify c [multi\_llid] <0-8>

#### 6.Pon number(s)

modify c [active\_pon] <0-8>

#### 7.Optical link protectio

modify c [holdover] <0-65535>

#### 8.Onu management IP address

modify c [mgmt] ip <A.B.C.D> mask <A.B.C.D> {[gw] <A.B.C.D>}\*1 {[cvlan] <1-4095>}\*1 {[svlan] <1-4095>}\*1 {[pri] <0-7>}\*1

#### 9. Onu SNMP parameters

```
modifyctc [mdu_snmp] v2 host <A.B.C.D> trap-port <1-65535> snmp-port <1-65535>
name <string> {[com_rd] <string>}*1 {[com_wr] <string>}*1
```

### 10. Onu SLA management

```
modifyctc [sla] [disable]
modifyctc [sla] [enable] [sp_basic]
modify ctc [sla] [enable] [wrr|sp_wrr] {queue <1-8> fix_packet_size <0-1900>
fix_bandwidth <0-1024> guaranteed-bandwidth <1-1024> best_effort_bandwidth <1-1024>
weight <0-100>}*8
```

### 11. Onuport flow control

```
modifyctc eth <1-255> [pause] [enable|disable]
```

### 12. Onu port loop detection

```
modifyctc eth <1-255> [loopdetect] [enable|disable]
```

### 13. Onu port multicast vlan strip

```
modifyctc eth <1-255> [mc_tagstrip] [enable|disable]
modify ctc eth <1-255> [mc_tagstrip] [iptv] set {<1-4095> to <1-4095>}*4
```

### 14. Onu port phy

```
modifyctc eth <1-255> [phy_ctrl] [enable|disable]
```

### 15. Onu port adaptive

```
modifyctc eth <1-255> [autoneg] [enable|disable]
```

### 16. Onu port maximum number of multicast groups

```
modifyctc eth <1-255> [mc_maxgrp] <0-4096>
```

### 17. Onu port ingress ratelimit

```
modifyctc eth <1-255> [policy] cir <1-1048576> [cbs] <1-10240> [ebs] <1-10240>
modifyctc eth <1-255> [policy] default
```

### 18. Onu port egress ratelimit

```
modifyctc eth <1-255> [rate_limit] cir <1-1048576> [pir] <1-1048576>
modifyctc eth <1-255> [rate_limit] default
```

### 19. Onu port vlan mode

```
modifyctc eth <1-255> [vlan] [mode] [transparent|tag|translation|aggregation|trunk]
modifyctc eth <1-255> [vlan] [default] <1-4095> {tpid <xxxx>}*1
modifyctc eth <1-255> [vlan] [translation] [set|add|del] {<1-4095> to <1-4095>}*8
modifyctc eth <1-255> [vlan] [trunk] [set|add|del] {<1-4095>}*8
modifyctc eth <1-255> [vlan] [aggregation] dst_vlan <1-4095> agg_vlan {<1-4095>}*8
```

### 20. Onu port multicast vlan

```
modify ctc eth <1-255> [mc_vlan] [add|del] {<1-4095>}*8
modify ctc eth <1-255> [mc_vlan] [clean]
```

### 21. Onu port classification&marking

```
modify ctc eth <1-255> [class] [add] precedence <1-8> priority <0-7> {[dst-mac]
[equal|unequal] <xx:xx:xx:xx:xx:xx>}*1 {[src-mac] [equal|unequal]
<xx:xx:xx:xx:xx:xx>}*1 {[vlan] [equal|unequal] <1-4094>}*1 {[cos] [equal|unequal]
<0-7>}*1 {[ether-type] [equal|unequal] <XXXX>}*1 {[src-ip] [equal|unequal]
<A.B.C.D>}*1 {[dest-ip] [equal|unequal] <A.B.C.D>}*1 {[protocol] [equal|unequal]
<0-255>}*1 {[tos-dscp] [equal|unequal] <0-255>}*1 {[src-port] [equal|unequal]
<0-65535>}*1 {[dest-port] [equal|unequal] <0-65535>}*1
```

```

modify ctc eth <1-255> [class] [clean]
modify ctc eth <1-255> [class] [del] precedence <1-8>

```

## 22. Onu wan connection(for HGU private)

```

modify pri [wan_conn] [add] [bridge] [internet|other]
modify pri [wan_conn] [add]
[route][internet|multicast|tr069|tr069_internet|tr069_voip|voip_internet|tr069_voip_internet|other] {nat [enable|disable]}*1
modify pri [wan_conn] [commit]
modify pri [wan_conn] [index] <1-8> [bridge] [internet|other]
modify pri [wan_conn] [index] <1-8> [delete]
modify pri [wan_conn] [index] <1-8> [dhcp]
modify pri [wan_conn] [index] <1-8> [pppoe] proxy [enable|disable] user <name>
pwd <password> server <name> mode [auto|payload]
modify pri [wan_conn] [index] <1-8> [qinq] [tpid] <1-65534> vlan <1-4085> {[cos]
<0-7>}*1
modify pri [wan_conn] [index] <1-8> [route]
[internet|multicast|tr069|tr069_internet|tr069_voip|voip_internet|tr069_voip_internet|other] {
nat [enable|disable]}*1
modify pri [wan_conn] [index] <1-8> [static] ip <A.B.C.D> mask <A.B.C.D> gw
<A.B.C.D> dns master <A.B.C.D> slave <A.B.C.D>
modify pri [wan_conn] [index] <1-8> [translation] [vlan] <1-4085> {<0-7>}*1
modify pri [wan_conn] [index] <1-8> [vlan] [tag|transparent] <1-4085> {<0-7>}*1
modify pri [wan_conn] [index] <1-8> [vlan|translation|qinq] [disable]

```

## 23. Onu WiFi service(for HGU private)

```

modify pri [wifi_ssid0|wifi_ssid1|wifi_ssid2|wifi_ssid3] [name] <string> hide
[enable|disable] auth_mode
[open|shared|wepauto|wpapsk|wpa|wpa2psk|wpa2|wpa/wpa2|wpapsk|wpa2psk|waipsk|wai]
encrypt_type [none|wep|tkip|aes|tkipaes|wpi]
modify pri [wifi_ssid0|wifi_ssid1|wifi_ssid2|wifi_ssid3] [radius] serverip type
[ipv4|ipv6|ipv4z|ipv6z|dns] len [1-255] ip <string> prefixlen <0-255> port <0-65535> key
<string>
modify pri [wifi_ssid0|wifi_ssid1|wifi_ssid2|wifi_ssid3] [wapi] type [ipv4|ipv6] serverip
<ipstring> port [1-65535]
modify pri [wifi_ssid0|wifi_ssid1|wifi_ssid2|wifi_ssid3] [wep] encryptionlevel [40|104]
keyindex <1-4> key1 <string> key2 <string> key3 <string> key4 <string>
modify pri [wifi_ssid0|wifi_ssid1|wifi_ssid2|wifi_ssid3] [wpa] shared_key <string>
rekey_interval <0-4194303>
modify pri [wifi_ssid0|wifi_ssid1|wifi_ssid2|wifi_ssid3] [commit|enable|disable]
modify pri [wifi_switch] [disable]
modify pri [wifi_switch] [enable] [FCC|ETSI] <0-1>
[80211b|80211g|80211bg|80211n|80211bgn] <0-20>

```

## 24. Onumac address aging time(private)

```

modify pri [age_time] <0-630>

```

## 25. Onu portmax mac addresses (private)

modify pri eth <1-255> [mac\_limit] <0-65535>

## 26. Onu port storm-control(private)

modify pri eth <1-255> [pkg\_suppress] broadcast <0-1024000> multicast <0-1024000> unknown <0-1024000>

## 27. Onu mac address aging time

modify ctc [agetime] <0-65535>

## 28. Onu optical link protection mechanism

modify ctc [pon\_protect] los\_optical <0-65535> los\_mpcp <0-65535>

## 29. Onu energy saving mode

modify ctc [power\_saving\_cfg] early\_wakeup [enable|disable] sleep\_duration\_max <0-65535>

modify ctc [sleep\_ctrl] sleep\_duration <0-65535> wake\_duration <0-65535> sleep\_flag [off|on|change] sleep\_mode [none|tx\_sleep\_only|tx\_and\_rx\_sleep]

## 30. Onu port loop

modify ctc eth <1-255> disableloop[enable|disable]

## 31. Onu port statistics

modify ctc eth [<1-255>] [monitor\_status] [enable|disable] <0-65535>

## 32. Onu port statistics clear

modify ctc eth [<1-255>] [monitor\_current]

## 33. Remove configuration

no

ctc[lan\_count|fast\_leave|fec\_mode|sla|holdover|mgmt|mdu\_snmp|active\_pon|mc\_switch|power\_saving\_cfg|pon\_protect|agetime|multi\_llid|sleep\_ctrl]

noctc eth<1-255>[pause|loopdetect|disableloop|monitor\_status|monitor\_current]

mc\_tagstrip|phy\_ctrl|autoneg|policy|rate\_limit|vlan|class|mc\_vlan|mc\_maxgrp]

no pri [age\_time|wifi\_switch|wifi\_ssid0|wifi\_ssid1|wifi\_ssid2|wifi\_ssid3|wan\_conn]

no pri eth <1-255> [pkg\_suppress|mac\_limit]

## VoIP template configuration

By default, there is an empty template, ID is 0, which you can't modify anything. When ONU is bound this empty template, all the parameters should be configured by specific command.

When ONU is configured by template and independent command at the same time, the independent command configured settings are effective.

	Command	Function
Step 1	<b>configure terminal</b>	Enter global configuration mode..
Step 2	<b>profile voip add</b> {<1-32767>}*1	Create the VoIP template
Step 3	<b>profile voip id</b> <1-32767>	Enter the VoIP template node
Step 4	<b>modify pots_count</b> <0-255>	Configure lan port quantity of template
Step 5	<b>commit</b>	Commit the template configuration
Step 6	<b>exit</b>	Exit template node

Step 7	<b>interface epon <i>slot/port</i></b>	Enter the pon interface configuration mode.
Step 8	<b>onu&lt;<i>onuid</i>&gt;profile voip id&lt;<i>1-32767</i>&gt;</b>	Binding the VoIP template to set correspondin
Step 9	<b>show onu&lt;<i>onuid</i>&gt;profile_id</b>	Query the onu binding template accordingly
Step 10	<b>exit</b>	Exit the pon interface node
Step 11	<b>show profile voip id&lt;<i>0-32767</i>&gt;</b>	Show template configuration
Step 12	<b>show profile voip id&lt;<i>0-32767</i>&gt;bind</b>	Show onu bindings in the template
Step 13	<b>no profile voip id&lt;<i>1-32767</i>&gt;</b>	Delete the VoIP template

VOIP template has the following configuration:

### 1.Onu pots port number(s)

modify [pots\_count] <0-255>

### 2.Onu voice global parameters

modify ctc [voip\_global\_param] [ip\_mode] [static] ipaddr <A.B.C.D> netmask <A.B.C.D> gateway <A.B.C.D>

modify ctc [voip\_global\_param] [ip\_mode] [dhcp]

modify ctc [voip\_global\_param] [ip\_mode] [pppoe] mode [auto|chap|pap] username <string> password <string>

modify ctc [voip\_global\_param] [vlan\_mode] [transparent|tag|vlan\_stacking] cvlan <0-4095> svlan <0-4095> priority <0-7>

### 3.Onu H. 248 protocol parameters

modify ctc [h248\_param\_config] [mg\_port] <1-65535> mgc\_ip <A.B.C.D> mgc\_port <1-65535> {bak\_mgc\_ip <A.B.C.D> bak\_mgc\_port <1-65535>}\*1

modify ctc [h248\_param\_config] [heartbeat] mode [disable|h248] cycle <1-65535> count <1-65535>

modify ctc [h248\_param\_config] [reg\_mode] [ip\_addr]

modify ctc [h248\_param\_config] [reg\_mode] [realm\_name|device\_name] mid <string>

### 4.Onu H. 248 RTP TID parameters

modify ctc [h248\_rtp\_tid] number <0-255> prefix <string>digit\_begin <0-4294967295><0-4294967295> mode [align|unaligned] digit\_length <0-255>

### 5.Onu SIP parameters

modify ctc [sip\_param\_config] [mg\_port] <1-65535> out\_bound\_serv ip <A.B.C.D> port <1-65535>

modify ctc [sip\_param\_config] [proxy\_serv] ip <A.B.C.D> port <1-65535>{bak\_ip <A.B.C.D> bak\_port <1-65535>}\*1

modify ctc [sip\_param\_config] [reg\_serv] ip <A.B.C.D> port <1-65535>{bak\_ip <A.B.C.D> bak\_port <1-65535>}\*1

modify ctc [sip\_param\_config] [heartbeat] switch [enable|disable] cycle <1-65535> count <1-65535> {reg\_interval <0-65535>}\*1

### 6.OnuFAX parameters

```

    modify etc [fax_modem_config] voice_t38 [enable|disable] control
[negotiation|auto_vbd]

```

#### 7. OnuSIP digitmap

```

modify etc [sip_digit_map] num <0-255><0-255><mapstr>

```

#### 8. OnuPOTS port userTID information

```

modify etc pots <1-255> [h248_user_tid] <name>

```

#### 9. OnuPOTS port user account information

```

modify etc pots <1-255> [sip_user_config] account <account> name <name> pwd
<password>

```

#### 10. Remove configuration instructions

```

no etc

```

```

[voip_global_param|h248_param_config|h248_rtp_tid|sip_param_config|fax_modem_conf
ig|sip_digit_map]

```

```

no etc pots <1-255> [h248_user_tid|sip_user_config]

```

### 18.8.4 Alarm threshold template configuration

Alarm threshold only can be configured by template. Begin at privileged configuration mode, configure alarm threshold template as the following table shows.

	<b>command</b>	<b>Function</b>
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>profile alarm add</b> {<1-32767>}*1	Create the alarm template
<b>Step 3</b>	<b>profile alarm id</b> <1-32767>	Enter the alarm template node
<b>Step 4</b>	<b>modify ...</b>	Configure alarm threshold template.
<b>Step 5</b>	<b>commit</b>	Commit the template configuration
<b>Step 6</b>	<b>exit</b>	Exit template node
<b>Step 7</b>	<b>interface epon</b> slot/port	Enter the pon interface configuration mode.
<b>Step 8</b>	<b>onu</b> <onuid> <b>profile alarm id</b> <1-32767>	Binding the alarm template to set corresponding.
<b>Step 9</b>	<b>show onu</b> <onuid> <b>profile id</b>	Query the onu binding template accordingly
<b>Step 10</b>	<b>exit</b>	Exit the pon interface node
<b>Step 11</b>	<b>show profile alarm id</b> <0-32767>	Show template configuration
<b>Step 12</b>	<b>show profile alarm id</b> <0-32767> <b>bind</b>	Show onu bindings in the template
<b>Step 13</b>	<b>no profile alarm id</b> <1-32767>	Delete the alarm template

Alarm template has the following configuration:

#### 1. Disable onu alarm

```

modify etc

```

```

[onu]

```

- [equipment\_alarm|power\_alarm|battery\_missing|battery\_failure|battery\_volt\_low|physical\_intrusion|onu\_self\_test\_failure|onu\_temp\_high\_alarm|onu\_temp\_low\_alarm|iad\_connection\_failure|pon\_if\_switch|sleep\_status\_update] [disable]
2. Enable/Disable onu alarm
- ```

modify                ctc                [onu]
[equipment_alarm|power_alarm|battery_missing|battery_failure|physical_intrusion|onu_self_test_failure|iad_connection_failure|pon_if_switch] [enable]

```
3. Enable/Disable & Clear onu temperature alarm
- ```

modify    ctc    [onu]    [onu_temp_high_alarm|onu_temp_low_alarm]    [enable]
<alarm><clear>

```
4. Enable/Disable onu voltage alarm
- ```

modify ctc [onu] [battery_volt_low] [enable] <0-65535><0-65535>

```
5. Disable/Enable pon alarm
- ```

modify                ctc
[pon][rx_power_high_alarm|rx_power_low_alarm|tx_power_high_alarm|tx_power_low_alarm|tx_bias_high_alarm|tx_bias_low_alarm|vcc_high_alarm|vcc_low_alarm|temp_high_alarm|temp_low_alarm|rx_power_high_warning|rx_power_low_warning|tx_power_high_warning|tx_power_low_warning|tx_bias_high_warning|tx_bias_low_warning|vcc_high_warning|vcc_low_warning|temp_high_warning|temp_low_warning] [disable]

```
6. Enable/Disable pon voltage alarm
- ```

modify ctc [pon] [vcc_high_alarm|vcc_low_alarm|vcc_high_warning|vcc_low_warning] [enable] <0-65535><0-65535>

```
7. Enable/Disable pon current alarm
- ```

modify                ctc
[pon][tx_bias_high_alarm|tx_bias_low_alarm|tx_bias_high_warning|tx_bias_low_warning] [enable] <0-65535><0-65535>

```
8. Enable/Disable pon tx & rx power alarm
- ```

modify                ctc
[pon][rx_power_high_alarm|rx_power_low_alarm|tx_power_high_alarm|tx_power_low_alarm|rx_power_high_warning|rx_power_low_warning|tx_power_high_warning|tx_power_low_warning] [enable] <0-65535><0-65535>

```
9. Enable/Disable pon temperature alarm
- ```

modify                ctc                [pon]
[temp_high_alarm|temp_low_alarm|temp_high_warning|temp_low_warning] [enable]
<alarm><clear>

```
10. Enable/Disable pon statistics alarm
- ```

modify ctc [pon] [downstream_drop_events_alarm|upstream_drop_events_alarm|downstream_crcerror_frames_alarm|downstream_undersize_frames_alarm|upstream_undersize_frames_alarm|downstream_oversize_frames_alarm|upstream_oversize_frames_alarm|downstream_fragments_alarm|downstream_jabbers_alarm|downstream_collisions_alarm|downstream_discard_frames_alarm|upstream_discard_frames_alarm|downstream_error_frames_alarm|downstream_drop_events_warning|upstream_drop_events_warning]

```

downstream\_crcerror\_frames\_warning|downstream\_undersize\_frames\_warning|upstream\_undersize\_frames\_warning|  
 downstream\_oversize\_frames\_warning|upstream\_oversize\_frames\_warning|downstream\_fragments\_warning|  
 downstream\_jabbers\_warning|downstream\_collisions\_warning|  
 downstream\_discard\_frames\_warning|upstream\_discard\_frames\_warning|  
 downstream\_error\_frames\_warning] {[disable]} [enable] <0-65535>}

### 12.Enable/Disable onu port alarm

modify ctc [eth] <1-255>  
 [eth\_port\_auto\_neg\_failure|eth\_port\_loss|eth\_port\_failure|eth\_port\_loopback|eth\_port\_congestion] [enable|disable]

### 13.Enable/Disable onu port statistics alarm

modify ctc [eth] <1-255>  
 [downstream\_drop\_events\_alarm|upstream\_drop\_events\_alarm|  
 downstream\_crcerror\_frames\_alarm|downstream\_undersize\_frames\_alarm|upstream\_undersize\_frames\_alarm|  
 downstream\_oversize\_frames\_alarm|upstream\_oversize\_frames\_alarm|downstream\_fragments\_alarm|  
 downstream\_jabbers\_alarm|downstream\_collisions\_alarm|  
 downstream\_discard\_frames\_alarm|upstream\_discard\_frames\_alarm|  
 downstream\_error\_frames\_alarm|status\_change\_times\_alarm|  
 downstream\_drop\_events\_warning|upstream\_drop\_events\_warning|  
 downstream\_crcerror\_frames\_warning|downstream\_undersize\_frames\_warning|upstream\_undersize\_frames\_warning|  
 downstream\_oversize\_frames\_warning|upstream\_oversize\_frames\_warning|downstream\_fragments\_warning|  
 downstream\_jabbers\_warning|downstream\_collisions\_warning|downstream\_discard\_frames\_warning|upstream\_discard\_frames\_warning|  
 downstream\_error\_frames\_warning|status\_change\_times\_warning] { [disable] |[enable] <0-65535>}

### 14.Enable/Disable pots alarm

modify ctc [pots] <1-64> [pots\_port\_failure] [enable|disable]

### 15.Enable/Disable el alarm

modify ctc [e1] <1-16> [e1\_port\_failure|e1\_timing\_unlock|e1\_loss] [enable|disable]

### 16.Remove configuration instructions

#### (1)Remove onu alarm configuration

no ctc [onu]  
 [equipment\_alarm|power\_alarm|battery\_missing|battery\_failure|battery\_volt\_low|physical\_intrusion|onu\_self\_test\_failure|onu\_temp\_high\_alarm|onu\_temp\_low\_alarm|iad\_connection\_failure|pon\_if\_switch|sleep\_status\_update]

#### (2)Removal pon alarm configuration

no ctc [pon]  
 [rx\_power\_high\_alarm|rx\_power\_low\_alarm|tx\_power\_high\_alarm|tx\_power\_low\_alarm|tx\_bias\_high\_alarm|tx\_bias\_low\_alarm|vcc\_high\_alarm|vcc\_low\_alarm|temp\_high\_alarm|temp\_low\_alarm|rx\_power\_high\_warning|rx\_power\_low\_warning|tx\_power\_high\_warning|tx\_power\_low\_warning|tx\_bias\_high\_warning|tx\_bias\_low\_warning|vcc\_high\_warning|vcc\_low\_warning|temp\_high\_warning|temp\_low\_warning]

```

no ctc [pon] [downstream_drop_events_alarm|upstream_drop_events_alarm|
downstream_crcerror_frames_alarm|downstream_undersize_frames_alarm|upstream_undersize_frames_alarm|downstream_oversize_frames_alarm|upstream_oversize_frames_alarm|downstream_fragments_alarm|
downstream_jabbers_alarm|downstream_collisions_alarm|
downstream_discard_frames_alarm|upstream_discard_frames_alarm|
downstream_error_frames_alarm|downstream_drop_events_warning|upstream_drop_events_warning|downstream_crcerror_frames_warning|downstream_undersize_frames_warning|upstream_undersize_frames_warning|
downstream_oversize_frames_warning|upstream_oversize_frames_warning|downstream_fragments_warning|downstream_jabbers_warning|downstream_collisions_warning|
downstream_discard_frames_warning|upstream_discard_frames_warning|
downstream_error_frames_warning]

```

(3) Remove port alarm configuration

```

no ctc [eth] <1-255>
[eth_port_auto_neg_failure|eth_port_loss|eth_port_failure|eth_port_loopback|eth_port_congestion]
no ctc [eth] <1-255> [downstream_drop_events_alarm|upstream_drop_events_alarm|
downstream_crcerror_frames_alarm|downstream_undersize_frames_alarm|upstream_undersize_frames_alarm|downstream_oversize_frames_alarm|upstream_oversize_frames_alarm|downstream_fragments_alarm|
downstream_jabbers_alarm|downstream_collisions_alarm|
downstream_discard_frames_alarm|upstream_discard_frames_alarm|
downstream_error_frames_alarm|status_change_times_alarm|
downstream_drop_events_warning|upstream_drop_events_warning|
downstream_crcerror_frames_warning|downstream_undersize_frames_warning|upstream_undersize_frames_warning|downstream_oversize_frames_warning|upstream_oversize_frames_warning|downstream_fragments_warning|
downstream_jabbers_warning|downstream_collisions_warning|
downstream_discard_frames_warning|upstream_discard_frames_warning|
downstream_error_frames_warning|status_change_times_warning]

```

(4) Remove pots port alarm configuration

```
no ctc [pots] <1-64> [pots_port_failure]
```

(5) Remove E1 port the alarm configuration

```
no ctc [e1] <1-16> [e1_port_failure|e1_timing_unlock|e1_loss]
```

### 18.8.5 Auto bind template in PON port

ONU register to OLT, user can set the template auto bind in the PON port.

|        | Command                         | Function                                    |
|--------|---------------------------------|---------------------------------------------|
| Step 1 | <b>configure terminal</b>       | Enter global configuration mode.            |
| Step 2 | <b>interface epon slot/port</b> | Enter the pon interface configuration mode. |

|                |                                                                                   |                                                     |
|----------------|-----------------------------------------------------------------------------------|-----------------------------------------------------|
|                | <b>Onu</b> <auto-bind> <b>profile</b><br>[dba srv voip alarm] <b>id</b> <0-32767> | Config the template auto bind to set corresponding. |
| <b>Step 3a</b> | <b>show</b> <onu><auto-bind> <b>profile_id</b>                                    | Show auto bind template.                            |

### 18.8.6 Show/Remove ONU template configuration

|                | <b>Command</b>                                                       | <b>Function</b>                   |
|----------------|----------------------------------------------------------------------|-----------------------------------|
| <b>Step 1</b>  | <b>configure terminal</b>                                            | Enter global configuration mode.. |
| <b>Step 2</b>  | <b>no profile {dba srv voip alarm}id</b><br><1-32767>                | Delete the template               |
| <b>Step 3a</b> | <b>show profile {dba srv voip alarm} all id</b><br><0-65535>}        | Show template configuration.      |
| <b>Step 3b</b> | <b>show profile {dba srv voip alarm} id</b><br><0-65535> <b>bind</b> | Show the template id binding onu  |

## 19. Controlling Switch Access with TACACS+

This section describes how to enable and configure TACACS+, which provides detailed accounting information and flexible administrative control over authentication and authorization processes. TACACS+ is facilitated through authentication, authorization, accounting (AAA) and can be enabled only through AAA commands.

### 19.1 Understanding TACACS+

TACACS+ is a security application that provides centralized validation of users attempting to gain access to your switch. TACACS+ services are maintained in a database on a TACACS+ daemon typically running on a UNIX or Windows NT workstation. You should have access to and should configure a TACACS+ server before the configuring TACACS+ features on your switch. TACACS+ provides for separate and modular authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service—authentication, authorization, and accounting—independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon. The goal of TACACS+ is to provide a method for managing multiple network access points from a single management service. Your switch can be a network access server along with other routers and access servers. A network access server provides connections to a single user, to a network or subnetwork, and to interconnected networks as shown in Figure 19-1.

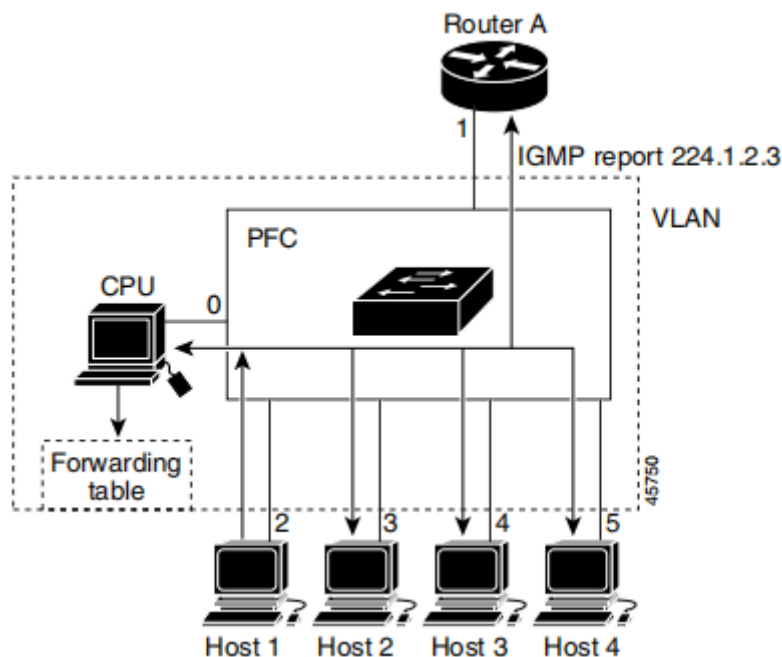


Figure 19-1 Typical TACACS+ Network Configuration

TACACS+, administered through the AAA security services, can provide these services:

- **Authentication**—Provides complete control of authentication through login and password dialog, challenge and response, and messaging support.  
The authentication facility can conduct a dialog with the user (for example, after a username and password are provided, to challenge a user with several questions, such as home address, mother's maiden name, service type, and social security number). The TACACS+ authentication service can also send messages to user screens. For example, a message could notify users that their passwords must be changed because of the company's password aging policy.
- **Authorization**—Provides fine-grained control over user capabilities for the duration of the user's session, including but not limited to setting autocommands, access control, session duration, or protocol support. You can also enforce restrictions on what commands a user can execute with the TACACS+ authorization feature.
- **Accounting**—Collects and sends information used for billing, auditing, and reporting to the TACACS+ daemon. Network managers can use the accounting facility to track user activity for a security audit or to provide information for user billing. Accounting records include user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

The TACACS+ protocol provides authentication between the switch and the TACACS+ daemon, and it ensures confidentiality because all protocol exchanges between the switch and the TACACS+ daemon are encrypted.

You need a system running the TACACS+ daemon software to use TACACS+ on your switch.

## 19.2 TACACS+ Operation

When a user attempts a simple ASCII login by authenticating to a switch using TACACS+, this process occurs:

1. When the connection is established, the switch contacts the TACACS+ daemon to obtain a username prompt, which is then displayed to the user. The user enters a username, and the switch then contacts the TACACS+ daemon to obtain a password prompt. The switch displays the password prompt to the user, the user enters a password, and the password is then sent to the TACACS+ daemon. TACACS+ allows a conversation to be held between the daemon and the user until the daemon receives enough information to authenticate the user. The daemon prompts for a username and password combination, but can include other items, such as the user's mother's maiden name.
2. The switch eventually receives one of these responses from the TACACS+ daemon:
  - **ACCEPT**—The user is authenticated and service can begin. If the switch is configured to require authorization, authorization begins at this time.

- REJECT—The user is not authenticated. The user can be denied access or is prompted to retry the login sequence, depending on the TACACS+ daemon.
  - ERROR—An error occurred at some time during authentication with the daemon or in the network connection between the daemon and the switch. If an ERROR response is received, the switch typically tries to use an alternative method for authenticating the user.
  - CONTINUE—The user is prompted for additional authentication information.  
After authentication, the user undergoes an additional authorization phase if authorization has been enabled on the switch. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.
- 2 If TACACS+ authorization is required, the TACACS+ daemon is again contacted, and it returns an ACCEPT or REJECT authorization response. If an ACCEPT response is returned, the response contains data in the form of attributes that direct the EXEC or NETWORK session for that user and the services that the user can access:
- Telnet, Secure Shell (SSH), rlogin, or privileged EXEC services
  - Connection parameters, including the host or client IP address, access list, and user timeouts

## 19.3 Configuring TACACS+

This section describes how to configure your switch to support TACACS+. At a minimum, you must identify the host or hosts maintaining the TACACS+ daemon and define the method lists for TACACS+ authentication. You can optionally define method lists for TACACS+ authorization and accounting. A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on a user. You can use method lists to designate one or more security protocols to be used, thus ensuring a backup system if the initial method fails. The software uses the first method listed to authenticate, to authorize, or to keep accounts on users; if that method does not respond, the software selects the next method in the list. This process continues until there is successful communication with a listed method or the method list is exhausted.

### 19.3.1 Default TACACS+ Configuration

TACACS+ and AAA are disabled by default.

To prevent a lapse in security, you cannot configure TACACS+ through a network management application. When enabled, TACACS+ can authenticate users accessing the switch through the CLI.

Note: Although TACACS+ configuration is performed through the CLI, the TACACS+ server authenticates HTTP connections that have been configured with a privilege level of 15.

### 19.3.2 Identifying the TACACS+ Server Host and Setting the Authentication

## Key

Begin at privileged configuration mode, follow these steps to identify the IP host or host maintaining TACACS+ server and optionally set the encryption key:

|        | Command                                                                                     | Function                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|---------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                                                   | Enter global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 2 | <b>tacacs-server host</b> <i>hostname</i>   <b>key</b> <i>string</i>   <b>console login</b> | Identify the IP host or hosts maintaining a TACACS+ server. Enter this command multiple times to create a list of preferred hosts. The software searches for hosts in the order in which you specify them. <ul style="list-style-type: none"> <li>• For <i>hostname</i>, specify the name or IP address of the host.</li> <li>• (Optional) For <i>key string</i>, specify the encryption key for encrypting and decrypting all traffic between the switch and the TACACS+ daemon. You must configure the same key on the TACACS+ daemon for encryption to be successful.</li> <li>• Enable tacacs authentication for console, default disable.</li> </ul> |
| Step 3 | <b>aaa new-model</b>                                                                        | Enable AAA.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 4 | <b>Show aaa</b>                                                                             | Verify your entries.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 5 | <b>Copy running-config</b><br><b>startup-config</b>                                         | (Optional) Save your entries in the configuration file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

To remove the specified TACACS+ server name or address, use the **no tacacs-server host** *hostname* global configuration command.

### 19.3.3 Configuring TACACS+ Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various ports. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific port before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named default). The default method list is automatically applied to all ports except those that have a named method list explicitly defined. A defined method list overrides the default method list. A method list describes the sequence and authentication methods to be queried to authenticate a user. You can 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 software uses the first method listed to

authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. 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.

Begin at privileged configuration mode, follow these steps to configure login authentication:

|        | Command                                                                    | Function                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                                  | Enter global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 2 | <b>aaa new-model</b>                                                       | Enable AAA.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 3 | <b>aaa authentication login {default   list-name} method1 [method2...]</b> | <p>Create a login authentication method list.</p> <ul style="list-style-type: none"> <li>• To create a default list that is used when a named list is not specified in the <b>login authentication</b> command, use the <b>default</b> keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all ports.</li> <li>• For list-name, specify a character string to name the list you are creating.</li> <li>• For method1..., specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails.</li> <li>• <b>group tacacs+</b>—Uses TACACS+ authentication. Before you can use this authentication method, you must configure the TACACS+ server. For more information, see the “Identifying the TACACS+ Server Host and Setting the Authentication Key” section</li> <li>• <b>local</b>—Use the local username database for authentication. You must enter username information in the database. Use the username password global configuration command.</li> </ul> |
| Step 4 | <b>Show aaa</b>                                                            | Verify your entries.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 5 | <b>Copy running-config startup-config</b>                                  | (Optional) Save your entries in the configuration file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

To disable AAA, use the **no aaa new-model global** configuration command. To disable AAA

authentication, use the **no aaa authentication login {default | list-name} method1 [method2...]** global configuration command.

### 19.3.4 Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the switch uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's session. The user is granted access to a requested service only if the information in the user profile allows it.

You can use the **aaa authorization** global configuration command with the **tacacs+** keyword to set parameters that restrict a user's network access to privileged EXEC mode.

The **aaa authorization exec tacacs+ local** command sets these authorization parameters:

- Use TACACS+ for privileged EXEC access authorization if authentication was performed by using TACACS+.
- Use the local database if authentication was not performed by using TACACS+.

Begin at privileged configuration mode, follow these steps to specify TACACS+ authorization for privileged EXEC access and network services:

|         | Command                                                                        | Function                                                                                                                                                                                                   |
|---------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | <b>configure terminal</b>                                                      | Enter global configuration mode.                                                                                                                                                                           |
| Step 2a | <b>aaa authorization commands</b><br><b>&lt;0-15&gt; default group tacacs+</b> | Enable authorization, 0 for login access (input username/password), 1 for enable mode, 15 for config mode.                                                                                                 |
| Step 2b | <b>aaa authorization exec default</b><br><b>group tacacs+</b>                  | Configure the switch for user TACACS+ authorization if the user has privileged EXEC access.<br><br>The <b>exec</b> keyword might return user profile information (such as <b>autocommand</b> information). |
| Step 3  | <b>Show aaa</b>                                                                | Verify your entries.                                                                                                                                                                                       |
| Step 4  | <b>Copy running-config</b><br><b>startup-config</b>                            | (Optional) Save your entries in the configuration file.                                                                                                                                                    |

To disable authorization, use the **no aaa authorization exec method1** global configuration command.

### 19.3.5 Starting TACACS+ Accounting

The AAA accounting feature tracks the services that users are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the switch

reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing.

Begin at privileged configuration mode, follow these steps to enable TACACS+ accounting for each Cisco IOS privilege level and for network services:

|               | <b>Command</b>                                                  | <b>Function</b>                                                                                                                                |
|---------------|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b>                                       | Enter global configuration mode.                                                                                                               |
| <b>Step 2</b> | <b>aaa accounting exec default<br/>start-stop group tacacs+</b> | Enable TACACS+ accounting to send a start-record accounting notice at the beginning of a privileged EXEC process and a stop-record at the end. |
| <b>Step 3</b> | <b>Show aaa</b>                                                 | Verify your entries.                                                                                                                           |
| <b>Step 4</b> | <b>Copy running-config<br/>startup-config</b>                   | (Optional) Save your entries in the configuration file.                                                                                        |

To disable accounting, use the **no aaa accounting {network | exec} {start-stop} method1...** global configuration command.

## 19.4 Displaying the TACACS+ Configuration

To display TACACS+ server statistics, use the **show aaa** privileged EXEC command.

## 20. System Management

### 20.1 Configuration file management

#### 20.1.1 Save configurations

After modified the configurations, you should save them so that these configurations can take effect next time it restarts. Use the following commands to save configurations.

|        | Command                   | Function                         |
|--------|---------------------------|----------------------------------|
| Step 1 | <b>configure terminal</b> | Enter global configuration mode. |
| Step 2 | <b>write</b>              | Save configurations.             |

#### 20.1.2 Erase configurations

If you need to reset to factory default, you can use the following commands to erase all configurations. After erased, the device will reboot automatically.

|        | Command                     | Function                         |
|--------|-----------------------------|----------------------------------|
| Step 1 | <b>configure terminal</b>   | Enter global configuration mode. |
| Step 2 | <b>erase startup-config</b> | Erase all configurations.        |

#### 20.1.3 Show startup configurations

Use the following command to display the configurations you have saved.

|        | Command                    | Function                         |
|--------|----------------------------|----------------------------------|
| Step 1 | <b>configure terminal</b>  | Enter global configuration mode. |
| Step 2 | <b>show startup-config</b> | Show all configurations.         |

#### 20.1.4 Show running configurations

Use the following commands to display running configurations. These running configurations may not be saved in flash.

|        | Command                    | Function                         |
|--------|----------------------------|----------------------------------|
| Step 1 | <b>configure terminal</b>  | Enter global configuration mode. |
| Step 2 | <b>show running-config</b> | Show running configurations.     |

#### 20.1.5 Upload/download configuration file

Use the following commands to upload configuration file to PC and download configuration file to device.

|                | <b>Command</b>                                                          | <b>Function</b>                                       |
|----------------|-------------------------------------------------------------------------|-------------------------------------------------------|
| <b>Step 1</b>  | <b>configure terminal</b>                                               | Enter global configuration mode.                      |
| <b>Step 2</b>  | <b>debug mode</b>                                                       | Enter debug mode                                      |
| <b>Step 3a</b> | <b>upload</b> <b>tftp</b><br><b>configuration</b> <filename><A.B.C.D>   | filename is Upgrade file<br>A.B.C.D is TFTP server IP |
| <b>Step 3b</b> | <b>download</b> <b>tftp</b><br><b>configuration</b> <filename><A.B.C.D> | filename is Upgrade file<br>A.B.C.D is TFTP server IP |

## 20.2 Check the system information

### 20.2.1 Check system running information

Use the following commands to view system information.

| <b>Command</b>            | <b>Function</b>      |
|---------------------------|----------------------|
| <b>show sys arp</b>       | Show ARP table       |
| <b>show sys cpu</b>       | Show CPU information |
| <b>show sys cpu-usage</b> | Show CPU usage rate  |
| <b>show sys mem</b>       | Show system memory   |
| <b>show sys ps</b>        | Show system process  |
| <b>show top</b>           | Show CPU utilization |
| <b>show task</b>          | Show thread name     |

### 20.2.2 Check version information

Use the following commands to check version information which includes hardware version, software version, software created time and so on.

|               | <b>Command</b>            | <b>Function</b>                  |
|---------------|---------------------------|----------------------------------|
| <b>Step 1</b> | <b>configure terminal</b> | Enter global configuration mode. |
| <b>Step 2</b> | <b>show version</b>       | Show version information.        |

### 20.2.3 Check system running time

Use the following command to show system running time after turned power on.

|               | <b>Command</b>               | <b>Function</b>                  |
|---------------|------------------------------|----------------------------------|
| <b>Step 1</b> | <b>configure terminal</b>    | Enter global configuration mode. |
| <b>Step 2</b> | <b>show sys running-time</b> | Show system running time.        |

## 20.3 System basic configurations

### 20.3.1 Configure system name

Use the following command to modify system name. This modification will take effect immediately. You will see it in command prompt prefix.

Begin at privileged configuration mode, configure system name as the following table shows.

|        | Command                   | Function                                            |
|--------|---------------------------|-----------------------------------------------------|
| Step 1 | <b>configure terminal</b> | Enter global configuration mode.                    |
| Step 2 | <b>hostname</b> <name>    | Configure system name. It must start with alphabet. |
| Step 3 | <b>hostname default</b>   | 恢复默认系统名                                             |

### 20.3.2 Configure terminal display attribute

This command is used to configure display line number when access by console port or telnet.

Begin at privileged configuration mode, configure terminal display attribute as the following table shows.

|        | Command                             | Function                                             |
|--------|-------------------------------------|------------------------------------------------------|
| Step 1 | <b>configure terminal</b>           | Enter global configuration mode.                     |
| Step 2 | <b>terminal length</b> <i>value</i> | Configure display line number. Value range is 0-512. |

### 20.3.3 Configure terminal time-out value

Use the following commands to configure terminal time-out value. Default value is 10 minutes.

|         | Command                                             | Function                                |
|---------|-----------------------------------------------------|-----------------------------------------|
| Step 1  | <b>configure terminal</b>                           | Enter global configuration mode.        |
| Step 2  | <b>line vty</b>                                     | Enter line node                         |
| Step 3a | <b>exec-timeout</b> <min> [ <i>&lt;second&gt;</i> ] | Set the command-line timeout            |
| Step 3b | <b>no exec-timeout</b>                              | Set the command-line timeout to default |
| Step 4  | <b>show exec-timeout</b>                            | Show the command-line timeout           |

## 20.4 System basic operations

### 20.4.1 Upgrade system

Use the following command to upgrade the equipment.

|         | Command                                                         | Function                         |
|---------|-----------------------------------------------------------------|----------------------------------|
| Step 1  | <b>configure terminal</b>                                       | Enter global configuration mode. |
| Step 2b | <b>download</b> <b>tftp</b><br><b>image</b> <filename><A.B.C.D> | Update firmware with header.     |

### 20.4.2 Network connectivity test

Use **ping** command to check network connectivity.

|        | Command                                | Function                                                |
|--------|----------------------------------------|---------------------------------------------------------|
| Step 1 | <b>configure terminal</b>              | Enter global configuration mode.                        |
| Step 2 | <b>ping</b> [-s<packet size>]<A.B.C.D> | <i>Packet size</i> is test packet length, unit is byte. |

### 20.4.3 Reboot system

Use the following command to reboot system.

|        | Command                   | Function                         |
|--------|---------------------------|----------------------------------|
| Step 1 | <b>configure terminal</b> | Enter global configuration mode. |
| Step 2 | <b>reboot</b>             | Reboot system.                   |

### 20.4.4 Telnet

You can telnet to system via outband or inband management IP. The default outband management IP is 192.168.8.100.

| Command                        | Function                                                                               |
|--------------------------------|----------------------------------------------------------------------------------------|
| <b>telnet 192.168.100</b>      | Telnet to application layer of system. Login name and password both are <b>admin</b> . |
| <b>telnet 192.168.100 2223</b> | Telnet to kernel of system. Login name is <b>default</b> .                             |
| <b>epon-olt(config)#switch</b> | Telnet to kernel of system. Login name is <b>default</b> .                             |

### 20.4.5 Configure RTC system time

Use the following command to configure RTC system time.

|        | Command                   | Function                         |
|--------|---------------------------|----------------------------------|
| Step 1 | <b>configure terminal</b> | Enter global configuration mode. |

|        |                                                                                                                                           |                         |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| Step 2 | <b>time set year</b> <2000-2099> <b>month</b> <1-12><br><b>day</b> <1-31> <b>hour</b> <0-23> <b>minute</b> <0-59><br><b>second</b> <0-59> | Configure the RTC clock |
| Step 3 | <b>show time</b>                                                                                                                          | Show the system time    |

### 20.4.6 Fan control

Use the following command to control fan running attribute.

|        | Command                           | Function                                                     |
|--------|-----------------------------------|--------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>         | Enter global configuration mode.                             |
| Step 2 | <b>fan temperature</b> <20-80>    | Configure Temperature of the fan                             |
| Step 3 | <b>fan mode</b> [open close auto] | Configure the fan open mode                                  |
| Step 4 | <b>show fan</b>                   | Show the fan configuration and current equipment temperature |

## 20.5 OAM debug information

### 20.5.1 Enable/disable OAM debug information

Use the following commands to enable or disable OAM debug information.

|        | Command                                                                                                                                                                                                                                       | Function                                                                                                                                                                                                                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                                                                                                                                                                                                     | Enter global configuration mode.                                                                                                                                                                                                                                                                                                                       |
| Step 2 | <b>debug mode</b>                                                                                                                                                                                                                             | Enter debug node                                                                                                                                                                                                                                                                                                                                       |
| Step 3 | <b>config level view</b><br>{ <b>recv_pkt</b>   <b>recv_from_onu_pkt</b>   <b>recv_from_cs8022_pkt</b>   <b>send_pkt</b>   <b>send_to_onu_pkt</b>   <b>send_to_cs8022_pkt</b>   <b>oam_pkt</b>   <b>oam_time</b> } { <b>on</b>   <b>off</b> } | On off :Open or close packet printing<br>recv_pkt:The received packets<br>recv_from_onu_pkt:receive packets from the onu<br>recv_from_cs8022_pkt:Receive packets from cs8022<br>send_pkt: Sent out oam packets<br>send_to_onu_pkt: Packets sent to the onu<br>send_to_cs8022_pkt: Packets sent to the cs800<br>oam_pkt:packets send and receive to ONU |

### 20.5.2 Enable/disable CPU debug information

Use the following commands to enable or disable CPU debug information.

|               | <b>Command</b>                      | <b>Function</b>                                                                                  |
|---------------|-------------------------------------|--------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b>           | Enter global configuration mode.                                                                 |
| <b>Step 2</b> | <b>debug mode</b>                   | Enter debug node.                                                                                |
| <b>Step 3</b> | <b>system debug {rx tx}{on off}</b> | On off : enable or disable CPU debug.<br>Rx: CPU receives packets.<br>Tx: CPU transmits packets. |

### 20.5.3 Enable/disable each function module debug information

Use the following commands to enable or disable function module debug information.

|               | <b>Command</b>                                                        | <b>Function</b>                                               |
|---------------|-----------------------------------------------------------------------|---------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b>                                             | Enter global configuration mode.                              |
| <b>Step 2</b> | <b>debug mode</b>                                                     | Enter debug node.                                             |
| <b>Step 3</b> | <b>system debug {acl timer port mac vlan vt igmp cfp qos}{on off}</b> | On off : enable or disable function module debug information. |

## 21. User Management

### 21.1 User privilege

There are two privileges for user, administrator user and normal user.

Normal user is a read-only user, only can view system information but not user information, configurations. Administrator user can view all information and configure all parameters.

### 21.2 Default user

By default, there is a administrator user **admin**, and password is **admin** too. Default user can't be deleted, modified, but you can modify its password.

### 21.3 Add user account

|        | Command                                                                                                             | Function                                                |
|--------|---------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                                                                           | Enter global configuration mode.                        |
| Step 2 | <b>user add</b> <i>user-name</i> <b>login-password</b><br><i>login-password</i>                                     | Add new user account.                                   |
| Step 3 | <b>user role</b> <i>user-name</i> { <b>admin</b>   <b>normal</b><br><b>enable-password</b> <i>enable-password</i> } | Specify user role. New user is a normal privilege user. |

### 21.4 Show user account list

|        | Command                   | Function                         |
|--------|---------------------------|----------------------------------|
| Step 1 | <b>configure terminal</b> | Enter global configuration mode. |
| Step 2 | <b>user list</b>          | Show user account list.          |

### 21.5 Delete user account

|        | Command                   | Function                         |
|--------|---------------------------|----------------------------------|
| Step 1 | <b>configure terminal</b> | Enter global configuration mode. |

|               |                                    |                      |
|---------------|------------------------------------|----------------------|
| <b>Step 2</b> | <b>user delete</b> <i>username</i> | Delete user account. |
|---------------|------------------------------------|----------------------|

## 21.6 Modify password

Every user can modify its own password while administrator user can modify other users' password. Modify password as the following table shows.

|               | <b>Command</b>                                                                                                                            | <b>Function</b>                               |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b>                                                                                                                 | Enter global configuration mode.              |
| <b>Step 2</b> | <b>user login-password</b> <i>user-name</i> <CR><br>Input new login password for user abc please.<br>New Password:<br>Confirm Password:   | Configure user's login password.              |
| <b>Step 3</b> | <b>user enable-password</b> <i>user-name</i> <CR><br>Input new enable password for user abc please.<br>New Password:<br>Confirm Password: | Configure user's configuration mode password. |

## 22. SNMP Configuration

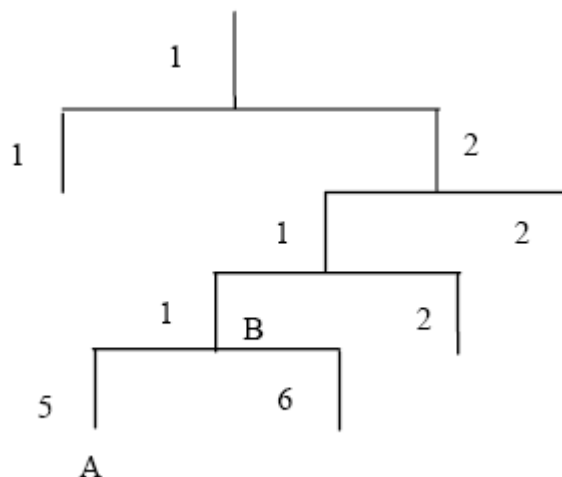
### 22.1 SNMP introduction

SNMP (Simple Network Management Protocol) is an extensive network management protocol at the moment. It is an industrial standard which is adopted and come into use for transmitting management information between two devices. Network administrator can search information, modify information, troubleshoot, diagnose fault, plan capacity and generate reports. SNMP adopts polling mechanism and provides basic functions, especially fits small, fast and low cost conditions. It is based on transport layer protocol UDP.

There are two parts of SNMP, NMS (Network Management Station) and agent. NMS is a station that runs client program, and agent is a server program that runs in device. NMS can send GetRequest, GetNextRequest and SetRequest messages to agent. Then agent will execute read or write command and respond to NMS. Agent also sends trap messages to NMS when device is abnormal.

### 22.2 SNMP version and MIB

In order to mark device's management variable uniquely, SNMP identifies management object by hierarchical structure name scheme. The set of objects is like a tree, which the node stands for management object, shown as the following picture.



MIB(Management Information Base), a set of device's variable definition, is used to describe the tree's hierarchical structure. For the management object B in above picture, we can use a string of numbers {1.2.1.1} to describe it uniquely. This string of numbers is Object Identifier.

GEAPON OLT series OLT support SNMP V1, V2C and V3. Common MIB shows in the following table.

| MIB attribute | MIB content            | Refer to |
|---------------|------------------------|----------|
| Public MIB    | MIB II based on TCP/IP | RFC1213  |
|               | RMON MIB               | RFC2819  |
|               | EthernetMIB            | RFC2665  |
| Private MIB   | VLAN MIB               |          |
|               | Device management      |          |
|               | Interface management   |          |

## 22.3 Configure SNMP

### 22.3.1 Configure community

Begin at privileged configuration mode, configure community as the following table shows.

|        | Command                                        | Function                                                                               |
|--------|------------------------------------------------|----------------------------------------------------------------------------------------|
| Step 1 | <b>config terminal</b>                         | Enter global configuration mode.                                                       |
| Step 2 | <b>snmp-server community</b> <word><br>[ro rw] | Configure SNMP community strings;                                                      |
| Step 3 | <b>show snmp-server community</b>              | Show the SNMP community configuration                                                  |
| Step 4 | <b>exit</b>                                    | From the global configuration mode to return to the privileged user configuration mode |
| Step 5 | <b>write</b>                                   | Save the configuration                                                                 |

### 22.3.2 Configure Trap the target host address

Use the following command to configure or remove the Trap messages of the target host IP address. Begin at privileged configuration mode, Configure Trap the target host address as the following table shows.

|         | Command                                                                                               | Function                                                                            |
|---------|-------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Step 1  | <b>config terminal</b>                                                                                | Enter global configuration mode.                                                    |
| Step 2a | <b>snmp-server host</b> <A.B.C.D>{udp-port<br><1-65535>}*1 {version [1 2c]}*1<br>{community <WORD>}*1 | Configure the Trap the target host address.<br>Configure the community string value |
| Step 2b | <b>no snmp-server host</b> < A.B.C.D > version<br>1 2c 3community                                     | Delete trap target host address.                                                    |

|         |                                         |                                   |
|---------|-----------------------------------------|-----------------------------------|
| Step 3a | <b>snmp-server enable traps snmp</b>    | Enable SNMP traps function        |
| Step 3b | <b>no snmp-server enable traps snmp</b> | Delete SNMP traps function        |
| Step 4  | <b>show snmp-server targetaddress</b>   | Check the SNMP trap configuration |
| Step 5  | <b>write</b>                            | Save the configuration            |

### 22.3.3 Configure Administrator ID and contact method

Begin at privileged configuration mode, Configure administrator ID and contact method as the following table shows.

|        | <b>Command</b>                    | <b>Function</b>                       |
|--------|-----------------------------------|---------------------------------------|
| Step 1 | <b>config terminal</b>            | Enter global configuration mode.      |
| Step 2 | <b>snmp-server contact</b> <line> | Configure contact string value        |
| Step 3 | <b>show snmp-server contact</b>   | Check the SNMP contact configuration. |
| Step 4 | <b>write</b>                      | Save the configuration.               |

### 22.3.4 Configure Ethernet switch location information

Begin at privileged configuration mode, Configure Ethernet switch location information as the following table shows.

|        | <b>Command</b>                     | <b>Function</b>                        |
|--------|------------------------------------|----------------------------------------|
| Step 1 | <b>config terminal</b>             | Enter global configuration mode        |
| Step 2 | <b>snmp-server location</b> <line> | Configure location string value        |
| Step 3 | <b>show snmp-server location</b>   | Check the SNMP location configuration. |
| Step 4 | <b>write</b>                       | Save the configuration.                |

## 23. Alarm and Event Management

### 23.1 Alarm and event introduction

If you enable alarm report, it will trigger alarm events when system occurred error or did some important operations. The alarm information will be save in a buffer, you can execute some commands such as show syslog to display. All the alarms can be sent to specific servier.

Alarms include fault alarm and recovery alarm. Fault alarm will not disappear until the fault is repaired and the alarm is cleared.

Events include running envents and security events, are notifications which generate and inform administrators under a normal condition. The difference between event and alarm is that event generates under a normal condition while alarm generates under an abnormal condition.

Command “show alarm-event information” is used to show description, level, type and class of all alarms and events.

### 23.2 Alarm management

Alarm severity level includes critical, major, minor and warning. Corresponding level in system log are alerts, critical, major and warnings. Alarm type includes device alarm, communication alarm and disposing alarm.

Device alarm contains low temperature, high temperature, CPU usage, memory usage, fan, PON, optical power and so on.

- Communication alarm contains port up/down, loopback, PON deregister, PON register failed, PON los, ONU deregister, illegal ONU register, ONU authorized failed, ONU MAC confliction, ONU LOID confliction, ONU link los, ONU dying gasp, ONU link fault, ONU link events, ONU extended OAM notification and so on.
- Dispoing alarm contains upgrade failed, upload configuration file failed, download configuration file failed and so on.

#### 23.2.1 System alarms

System alarms show the performance and security of system. The following table shows the system alarm list.

| System alarm | Reason                                    | Default |
|--------------|-------------------------------------------|---------|
| temp-high    | Device temperature higher than threshold. | disable |
| temp-low     | Device temperature lower than threshold.  | disable |

|                      |                                     |         |
|----------------------|-------------------------------------|---------|
| cpu-usage-high       | CPU usage higher than threshold.    | disable |
| mem-usage-high       | Memory usage higher than threshold. | disable |
| fan                  | Fan switch.                         | disable |
| download-file-failed | Download file failed                | enable  |
| upload-file-failed   | Upload file failed.                 | enable  |
| upgrade-file-failed  | Upgrade firmware failed.            | enable  |
| port-updown          | Port link up and link down.         | enable  |
| port-loopback        | Port loopback.                      | disable |

|         | Command                                                                                                                           | Function                                                                                                                           |
|---------|-----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | <b>configure terminal</b>                                                                                                         | Enter global configuration mode.                                                                                                   |
| Step 2a | <b>alarm</b><br><b>{temp-high temp-low cpu-usage-high mem-usage-high} disable</b>                                                 | Disable system alarm report.                                                                                                       |
| Step 2b | <b>alarm</b><br><b>{temp-high temp-low cpu-usage-high mem-usage-high} enable</b><br><i>&lt;alarm-value&gt;&lt;clear-value&gt;</i> | Enable system alarm report and configure system alarm threshold.<br>alarm-value: alarm threshold.<br>clear-value: clear threshold. |
| Step 2c | <b>alarm</b><br><b>{fan port-updown port-loopback register-failed deregister}{enable disable}</b>                                 | Enable or disable system alarm report.                                                                                             |
| Step 3  | <b>show alarm configuration</b>                                                                                                   | Show system alarm configurations.                                                                                                  |

### 23.2.2 PON alarms

Get rid of the issue caused by PON port or fiber by monitoring PON alarms, ensure PON works well. The following table shows PON alarm list.

| PON alarm        | Reason                                             | Default |
|------------------|----------------------------------------------------|---------|
| pon-txpower-high | PON port transmitting power higher than threshold. | enable  |
| pon-txpower-low  | PON port transmitting power lower than threshold.  | enable  |
| pon-txbias-high  | PON port bias current higher than threshold.       | enable  |

|                 |                                             |         |
|-----------------|---------------------------------------------|---------|
| pon-txbias-low  | PON port bias current lower than threshold. | enable  |
| pon-vcc-high    | PON port voltage higher than threshold.     | enable  |
| pon-vcc-low     | PON port voltage lower than threshold.      | enable  |
| pon-temp-high   | PON port temperature higher than threshold. | enable  |
| pon-temp-low    | PON port temperature lower than threshold.  | enable  |
| pon-los         | Fiber unconnected or link fault.            | enable  |
| deregister      | PON deregister.                             | disable |
| register-failed | PON register failed.                        | enable  |

Configure global PON alarm as the following table shows.

|         | Command                                                                                                                                                              | Function                                 |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| Step 1  | <b>configure terminal</b>                                                                                                                                            | Enter global configuration mode.         |
| Step 2a | <b>alarm</b><br><b>{pon-register-failed pon-deregister}{enable disable}</b>                                                                                          | Enable or disable PON alarm report.      |
| Step 2a | <b>alarm</b><br><b>{pon-txpower-high pon-txpower-low pon-txbias-high pon-txbias-low pon-vcc-high pon-vcc-low pon-temp-high pon-temp-low pon-los}{enable disable}</b> | Enable or disable PON port alarm report. |
| Step 3  | <b>show alarm configuration</b>                                                                                                                                      | Show alarm configurations.               |

Configure PON port alarm as the following table shows. Before this, you must enable global PON alarm. By default, global PON alarm is enabled, the alarms will be record in system log.

|         | Command                                                                                                                            | Function                                                     |
|---------|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| Step 1  | <b>configure terminal</b>                                                                                                          | Enter global configuration mode.                             |
| Step 2  | <b>interface epon <i>slot/port</i></b>                                                                                             | Enter PON interface configuration mode.                      |
| Step 3a | <b>alarmpon</b><br><b>optical{tx_power_high tx_power_low tx_bias_high tx_bias_low vcc_high vcc_low temp_high temp_low} disable</b> | Disable PON port alarm report.                               |
| Step 3b | <b>alarm pon optica</b><br><b>{tx_power_high tx_power_low</b><br><b> tx_bias_high  tx_bias_low vcc_high</b>                        | Enable PON port alarm report and configure alarm parameters. |

|               |                                                                                              |                                                                |
|---------------|----------------------------------------------------------------------------------------------|----------------------------------------------------------------|
|               | <code> vcc_low   temp_high temp_low}enable<br/>&lt;alarm-value&gt;&lt;clear-value&gt;</code> | alarm-value: alarm threshold.<br>clear-value: clear threshold. |
| <b>Step 4</b> | <b>show alarm pon optical configuration</b>                                                  | Show PON port alarm configurations.                            |

#### ONU alarms

ONU alarms also can help administrator to get rid of some ONU fault. The following table shows ONU alarm list.

| ONU alarm            | Reason                                                                                  | Default |
|----------------------|-----------------------------------------------------------------------------------------|---------|
| onu-deregister       | ONU deregister                                                                          | enable  |
| onu-link-lost        | ONU fiber unconnected or link fault.                                                    | disable |
| onu-illegal-register | Illegal ONU register.                                                                   | enable  |
| onu-auth-failed      | ONU LOID authorized failed in auto authorization mode or failed caused by packets loss. | enable  |
| onu-mac-conflict     | Current PON port exist MAC conflict with authorized ONU in the system.                  | enable  |
| onu-loid-conflict    | Current PON port exist LOID conflict with authorized ONU in the system.                 | enable  |
| onu-critical-event   | ONU critical link event.                                                                | enable  |
| onu-dying-gasp       | ONU power down.                                                                         | enable  |
| onu-link-fault       | ONU link fault.                                                                         | enable  |
| onu-link-event       | ONU link event                                                                          | disable |
| onu-event-notific    | ONU extended OAM notification                                                           | enable  |

|               | Command                                                                                                                                                                                                                    | Function                            |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b>                                                                                                                                                                                                  | Enter global configuration mode.    |
| <b>Step 2</b> | <b>alarm<br/>{onu-deregister onu-link-lost onu-illegal-register onu-auth-failed onu-mac-conflict onu-loid-conflict onu-critical-event onu-dying-gasp onu-link-fault onu-link-event onu-event-notific} {enable disable}</b> | Enable or disable ONU alarm report. |
| <b>Step 3</b> | <b>show alarm configuration</b>                                                                                                                                                                                            | Show system alarm configurations.   |

## 23.3 Event management

Event severity level includes critical, major, minor and warning. Corresponding level in system log are alerts, critical, major, warnings. Event type includes device event, communication event and disposing event.

- Device event contains device reboot, PON event and so on.
- Communication event contains PON register, PON los recovery, ONU register, ONU find, ONU authorized successful, ONU deregister successful and so on.
- Disposing event contains save configuration event, erase configuration event, download configuration file successful, upload configuration file successful, upgrade successful and so on.

### 23.3.1 System events

System events are mainly used to monitor performance and security of system, ensure system works well.

| System event          | Reason                       | Default |
|-----------------------|------------------------------|---------|
| reset                 | Device reset.                | disable |
| config-save           | Save configuration.          | enable  |
| config-erase          | Erase configuration.         | enable  |
| download-file-success | Download file successful.    | enable  |
| upload-file-success   | Upload file successful.      | enable  |
| upgrade-file-success  | Upgrade firmware successful. | enable  |

|         | Command                             | Function                               |
|---------|-------------------------------------|----------------------------------------|
| Step 1  | <b>configure terminal</b>           | Enter global configuration mode.       |
| Step 2a | <b>event reset {enable disable}</b> | Enable or disable system event report. |
| Step 3  | <b>show event configuration</b>     | Show system event configurations.      |

### 23.3.2 PON events

Get rid of the issue caused by PON port or fiber by monitoring PON events, ensure PON works well. The following table shows PON event list.

| PON event        | Reason            | Default |
|------------------|-------------------|---------|
| pon-register     | PON register.     | disable |
| pon-los-recovery | PON los recovery. | enable  |

|               | <b>Command</b>                                               | <b>Function</b>                     |
|---------------|--------------------------------------------------------------|-------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b>                                    | Enter global configuration mode.    |
| <b>Step 2</b> | <b>event {pon-register pon-los-recovery}{enable disable}</b> | Enable or disable PON event report. |
| <b>Step 3</b> | <b>show event configuration</b>                              | Show system event configurations.   |

### 23.3.3 ONU events

ONU events also can help administrator to get rid of some ONU fault. The following table shows ONU event list.

| <b>ONU event</b>   | <b>Reason</b>                    | <b>Default</b> |
|--------------------|----------------------------------|----------------|
| onu-register       | ONU register.                    | enable         |
| onu-link-discover  | ONU discover.                    | disable        |
| onu-auth-success   | OLT authorizes ONU successful.   | enable         |
| onu-deauth-success | OLT deauthorizes ONU successful. | disable        |

|                | <b>Command</b>                                                                                    | <b>Function</b>                     |
|----------------|---------------------------------------------------------------------------------------------------|-------------------------------------|
| <b>Step 1</b>  | <b>configure terminal</b>                                                                         | Enter global configuration mode.    |
| <b>Step 2b</b> | <b>event {onu-register onu-link-discover onu-auth-success onu-deauth-success}{enable disable}</b> | Enable or disable ONU event report. |
| <b>Step 3</b>  | <b>show event configuration</b>                                                                   | Show system event configuration.    |

## 24.OAM Interactive Information Management

OAM interactive information records whole process of ONU register, OAM discovery and CTC management. Complete log information can help administrator to know ONU register status and find out abnormal information. The log information come from all running module of EPON system.

Log of main functions are: monitoring equipment running status, tracking some applications provide abundant and valuable information.Can help us to fault location, troubleshooting and network security management.

### 23.1 Configure log output level of modules

|        | Command                                                                                                                                                                         | Function                           |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
| Step 1 | <b>configure terminal</b>                                                                                                                                                       | Enter global configuration mode.   |
| Step 2 | <b>debug mode</b>                                                                                                                                                               | Enter debug node                   |
| Step 3 | <b>config level print</b><br>{all osal timer interrupt cpuload malloc init aal app cli sc oam hello dba pkt_header pkt_content event l2ftp pkt system others ess ess_vlan}<0-7> | Configure modules log output level |
| Step 4 | <b>display level print</b><br>{all osal timer interrupt cpuload malloc init aal app cli sc oam hello dba pkt_header pkt_content event l2ftp pkt system others ess ess_vlan}     | Show modules log output level      |

### 23.2 Configure log store level of modules

|        | Command                                                                                                                                                                              | Function                                 |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| Step 1 | <b>configure terminal</b>                                                                                                                                                            | Enter global configuration mode.         |
| Step 2 | <b>debug mode</b>                                                                                                                                                                    | Enter debug node                         |
| Step 3 | <b>config level</b><br><b>log</b> {all osal timer interrupt cpuload malloc init aal app cli sc oam hello dba pkt_header pkt_content event l2ftp pkt system others ess ess_vlan}<0-7> | Configure modules log memory store level |
| Step 4 | <b>display level log</b>                                                                                                                                                             | Show modules log memory                  |

|                |                                                                                                                                                              |                                                                          |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
|                | <b>{all osal timer interrupt cpuload malloc init aal app cli sc oam hello dba pkt_header pkt_content event l2ftp pkt system others ess_vlan}</b>             | store level                                                              |
| <b>Step 5a</b> | <b>display log {all osal timer interrupt cpuload malloc init aal app cli sc oam hello dba pkt_header pkt_content event l2ftp pkt system others ess_vlan}</b> | Display module stored in the memory of the log information               |
| <b>Step 5b</b> | <b>display log level &lt;0-7&gt;</b>                                                                                                                         | Display log information stored in the memory module at all levels        |
| <b>Step 5c</b> | <b>display log {latest oldest} &lt;1-1024&gt;</b>                                                                                                            | Display log information                                                  |
| <b>Step 6a</b> | <b>delete log {all osal timer interrupt cpuload malloc init aal app cli sc oam hello dba pkt_header pkt_content event l2ftp pkt system others ess_vlan}</b>  | Delete all modules are stored in the memory of the log information       |
| <b>Step 6b</b> | <b>delete log level &lt;0-7&gt;</b>                                                                                                                          | Delete all the log information stored in the memory module at all levels |

## 25. System Log

### 24.1 System log introduction

System log is mainly used to record running condition and user operant behavior of the whole system. It is helpful for administrator to know and monitor system working condition, record abnormal information. System log comes from all the running module of system. Log system gather, manage, save and display the information. It can be shown in the device when you need to debug or check system status, and also can be sent to a server for long-term running status and operation tracking.

#### 24.1.1 Log type

System log has five types:

- **Abnormal information log**  
Abnormal information log mainly records the abnormal phenomenon of each module, such as abnormal response, inside state machine error, key process execute error and so on.
- **Alarm log**  
Alarm log mainly records the information from alarm module. Critical alarm, major alarm, minor alarm and warning are corresponding with alerts, critical, major, warnings log level respectively.
- **Event log**  
Event log mainly records the information from event module. Critical event, major event, minor event and warning are corresponding with alerts, critical, major, warnings log level respectively.
- **Operation log**  
Operation log mainly records the informations from CLI and SNMP.
- **Debug log**  
Debug log mainly records the information from networking debugging, such as received IGMP messages, RSTP BPDU messages, state machine skip and so on.

#### 24.1.2 System log level

Syslog information level reference:

| Log level     | Log contrast                            |
|---------------|-----------------------------------------|
| 7:emergencies | Abnormal log                            |
| 6:alerts      | Alarm/event log(urgent)<br>Abnormal log |
| 5:critical    | Alarm/event log(major)<br>Abnormal log  |

|                 |                                          |
|-----------------|------------------------------------------|
| 4:major         | Alarm/event log(minor)<br>Abnormal log   |
| 3:warnings      | Alarm/event log(warning)<br>Abnormal log |
| 2:notifications | Operation log                            |
| 1:informational | Operation log                            |
| 0:debugging     | Debug log                                |

## 24.2 Configure system log

### 24.2.1 Show system log

|        | Command                                                                                                      | Function                                      |
|--------|--------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| Step 1 | <b>configure terminal</b>                                                                                    | Enter global configuration mode.              |
| Step 2 | <b>Show</b> <b>syslog[level</b><br><b>{debug info notice warning major critical </b><br><b>alert emerg}]</b> | Show all system log or log of specific level. |

### 24.2.2 Clear system log

|        | Command                                                                                                       | Function                                       |
|--------|---------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                                                                     | Enter global configuration mode.               |
| Step 2 | <b>Clear</b> <b>syslog[level</b><br><b>{debug info notice warning major critical </b><br><b>alert emerg}]</b> | Clear all system log or log of specific level. |

### 24.2.3 Configure system log server

|         | Command                                                                              | Function                                 |
|---------|--------------------------------------------------------------------------------------|------------------------------------------|
| Step 1  | <b>configure terminal</b>                                                            | Enter global configuration mode.         |
| Step 2a | <b>syslog server ip</b> <b>&lt;A.B.C.D&gt;</b> <b>port</b><br><b>&lt;1-65535&gt;</b> | Configure system log server IP and port. |
| Step 2b | <b>no syslog server</b>                                                              | Delete system log server configuration.  |
| Step 3  | <b>show syslog server</b>                                                            | Show system log server configuration.    |

### 24.2.4 Configure save level of system log

|        | Command                   | Function                         |
|--------|---------------------------|----------------------------------|
| Step 1 | <b>configure terminal</b> | Enter global configuration mode. |

|        |                                                                                     |                                                                 |
|--------|-------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| Step 2 | <b>syslog flash level</b><br>{debug info notice warning major critical alert emerg} | System log will be saved to flash if it is higher than you set. |
| Step 3 | <b>show syslog flash level</b>                                                      | Show system log level in flash.                                 |

#### 24.2.5 Save system log to flash

|        | <b>Command</b>            | <b>Function</b>                  |
|--------|---------------------------|----------------------------------|
| Step 1 | <b>configure terminal</b> | Enter global configuration mode. |
| Step 2 | <b>save syslog flash</b>  | Save system log to flash.        |

#### 24.2.6 Clear system log in flash

|        | <b>Command</b>            | <b>Function</b>                  |
|--------|---------------------------|----------------------------------|
| Step 1 | <b>configure terminal</b> | Enter global configuration mode. |
| Step 2 | <b>clear syslog flash</b> | Clear system log in flash.       |

#### 24.2.7 Upload system log

|        | <b>Command</b>                                            | <b>Function</b>                          |
|--------|-----------------------------------------------------------|------------------------------------------|
| Step 1 | <b>configure terminal</b>                                 | Enter global configuration mode.         |
| Step 2 | <b>upload tftp syslog &lt;filename&gt;&lt;A.B.C.D&gt;</b> | Upload system log to local host by TFTP. |