# GEPON OLT

# CLI USER MANUAL

Version V1.5

Release Date 2018-6-1

**Content**

# 1. Access to OLT

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

1. Connect PC to OLT console port by console cable.
2. Run hypeterminal 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 truned on the power, there is boot information printing. After startup, press enter and input username and password to login.

Notice:

*The default username and password of CLI both are admin. For example,*

*Login: admin*

*Password: admin*

*epon-olt> enable*

*Password: admin*

*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 charpter.

# 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 specialties, 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# | | **exit** |
| Global configuration mode | Configure system parameters | epon-olt(config)# | **configure terminal** | **exit** |
| Interface configuration mode | Configure interface parameters | epon-olt(config-if)# | **interface** *{interface_type slot/port}* | **exit** |

## 2.3 CLI specialities

### 2.3.1 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 sring.

```
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.

### 2.3.2 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 |

### 2.3.3 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 | **history** | 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. |

### 2.3.4 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 |

### 2.3.5 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><br>Down direction key↓or <Ctrl+N> | Display history command. |
| Tab key | Input incomplete key words end with Tab key, CLI will provide partly help.<br>If it is unique, the key word which matches what you input will be used and display in another row.<br>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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface***{interface_type slot/port}* | 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface***{interface_type slot/port}* | Enter interface configuration mode. |
| **Step 3a** | **no shutdown** | Enable port |

| | | |
|---|---|---|
| **Step 3b** | **shutdown** | Disable port. |
| **Step 4** | **exit** | Exit to gloable configuration mode. |
| **Step 5** | **show interface***{interface_type slot/port}* | Show interface configurations. |
| **Step 6** | **write** | 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.

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface***{interface_type slot/port}* | Enter interface configuration mode. |
| **Step 3a** | **duplex { auto \| full \| half }** | Configure port duplex mode. |
| **Step 3b** | **no duplex** | Reset duplex mode to default. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show interface***{interface_type slot/port}* | Show interface configurations. |
| **Step6** | **write** | 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface***{interface_type slot/port}* | Enter interface configuration mode. |
| **Step 3a** | **speed { 10 \| 100 \| 1000 \| auto }** | Configure port speed. |
| **Step 3b** | **no speed** | Reset port speed to default. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show interface***{interface_type slot/port}* | Show interface configurations. |
| **Step 6** | **write** | 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface***{interface_type slot/port}* | Enter interface configuration mode. |
| **Step 3a** | **line-rate {ingress \| egress} bps** *value* | Configure port rate limitation. Value range: 64-1000000, it should be integral multiple of 64kbps. |
| **Step 3b** | **no line-rate {ingress \| egress}** | Delete port rate limitation configurations. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show interface***{interface_type slot/port}* | Show interface configurations. |
| **Step6** | **write** | 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.

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

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface** *{interface_type slot/port}* | Enter interface configuration mode. |
| **Step 3a** | **switchporthybridvlan** *vlan_id* **{tagged \| untagged}** | Add specific VLAN to hybrid port. |
| **Step 3b** | **switchport hybrid transparent** | Set port VLAN mode as transparent. OLT will add 1~4094 VLAN to the port. This operation will take about 3 minutes. |
| **Step 3c** | **no switchport hybrid vlan** *vlan_id* | Remove VLAN from port. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show interface** *{interface_type slot/port}* | Show interface configurations. |
| **Step 6** | **write** | 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** | **configure terminal** | Enter global configuration |
| **Step 2** | **interface** *{interface_type slot/port}* | Enter interface configuration |
| **Step 3a** | **switchporttrunkvlan** *vlan_id* | Add specific VLAN to trunk port. VLAN mode is tagged. |
| **Step 3b** | **no switchport trunk vlan** *vlan_id* | Remove VLAN from port. |
| **Step 5** | **exit** | Exit to global configuration mode. |
| **Step 6** | **show interface** *{interface_type slot/port}* | Show interface configurations. |
| **Step 7** | **write** | 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** | **configure terminal** | Enter global configuration. |
| **Step 2** | **interface***{interface_type slot/port}* | Enter interface configuration mode. |
| **Step 3a** | **switchport{hybrid\|trunk}pvid vlan***vlan_id* | Configure hybrid mode or trunk mode port PVID. |
| **Step 3b** | **no switchport{hybrid\|trunk}pvid** | Reset hybrid or trunk port PVID to default. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show interface***{interface_type slot/port}* | Show interface configurations. |
| **Step 6** | **write** | 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface***{interface_type slot/port}* | Enter interface configuration mode. |
| **Step 3a** | **switchportaccess vlan***vlan_id* | Configure access port VLAN. |
| **Step 3b** | **no switchportaccess vlan** | Reset access port VLAN to default. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show interface***{interface_type slot/port}* | Show interface configurations. |
| **Step 6** | **write** | Save configurations. |

### 3.1.12 Configure port flow control

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

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface***{interface_type slot/port}* | Enter interface configuration mode. |
| **Step 3a** | **flowcontrol on** | Enable flow control function. |
| **Step 3b** | **no flowcontrol** | Disable flow control function. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show interface***{interface_type slot/port}* | Show interface configurations. |
| **Step 6** | **write** | 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface***{interface_type slot/port}* | Enter interface configuration mode. |
| **Step 3a** | **storm-control broadcast pps***value* | Configure broadcast suppression.<br>Value range: 64-1000000, it should be integral multiple of 64kbps. |

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

### 3.1.14 Configure port multicast suppression

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

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

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

| | | |
|---|---|---|
| **Step 4** | **exit** | Exit global configuration mode. |
| **Step 5** | **show interface** *{interface_type slot/port}* | Show interface configurations. |
| **Step 6** | **write** | 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.

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

### 3.1.17 Configure port loopback

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

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2a** | **loopback detect enable** | Enable port loopback detection. |
| **Step 2b** | **no loopback detect** | Disable port loopback detection. |
| **Step 3** | **show loopback detect** | Show port loopback detection status. |
| **Step 4** | **exit** | 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.

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

### 3.1.20 Show port statistics

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface** *{interface_type slot/port}* | Enter interface configuration mode. |

| | | |
|---|---|---|
| **Step 3** | **show statistics** | Show port statistics. |
| **Step 4** | **exit** | Exit to global configuration mode. |

### 3.1.21 Clean port statistics

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **show interface***{interface_type slot/port}* | Show port statistics. |
| **Step 3** | **clean statistics** | Clean port statistics. |

### 3.1.22 Show interface configurations

| Operation | **Command** |
|---|---|
| Show interface configurations. | **Show interface** *{interface_type slot/port}* |

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
        Unknow 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

## 3.2 Example

Configure VLAN and broadcast suppresstion 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.

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2a** | **channel-group** *<1-4>***mode static** | Create static aggregation group. |
| **Step 2b** | **no channel-group** *<1-4>* | Delete static aggregation group. |
| **Step 3** | **show channel-group summary** | 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.

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **channel-group** *<1-4>***load-balance {smac\|dmac\|sdmac\|sip\|dip\|sdip}** | Specify which link is used to transmit traffic in aggregation group. |
| **Step 3** | **show channel-group summary** | Show aggregation configurations. |

### 4.2.3 Configure member port of aggregation group

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

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

### 5.1.2 Configure/delete VLAN description

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface vlan** *vlan_id* | Create VLAN or enter VLAN infterface configuration mode. VLAN ID range is from 1 to 4094. |

| | | |
|---|---|---|
| **Step 3a** | **description** *string* | Configure VLAN description. |
| **Step 3b** | **no description** | Delete VLAN description. |
| **Step 4** | **exit** | Exit to bloble configuration mode. |
| **Step 5** | **show interface vlan** *vlan_id* | Show VLAN interface information. |
| **Step 6** | **write** | 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.

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

## 5.2 Show VLAN information

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

| **Operation** | **Command** |
|---|---|
| Show VLAN information | **show interface vlan** |
| Show VLAN port members | **show interface vlan***vlan-id* |

**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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface***{interface_type slot/port}* | Enter interface configuration mode. |
| **Step 3a** | **dot1q-tunnelvlan-maping***ori_vlan* **{any|** *ori_vlan_pri***}** *tra_vlani* **{any|tra_vlan_pri} {db-tag|one-tag}** | Configure VLAN translation/QinQ.<br>db-tag means QinQ.<br>one-tag means translation. |
| **Step 3b** | **no dot1q-tunnelvlan-maping***ori_vlantra_vlanid* | Delete VLAN translation/QinQ. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show vlanvlan-maping interface** *{interface_type slot/port}* | Show VLAN translation/QinQ configurations. |
| **Step 6** | **write** | 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 proccess 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.

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2a** | **mac address-table static vlan** *vlan_idxxxx:xxxx:xxxx* **interface** *interface_type slot/port* | Add static MAC address entry. |
| **Step 2b** | **no mac address-table vlan***vlan_id xxxx:xxxx:xxxx* | Delete MAC address entry. |
| **Step 2c** | **mac address-table clean** | Clean MAC address table. |

| | | |
|---|---|---|
| **Step 3** | **show mac address-table** | Show MAC address table. |
| **Step 4** | **write** | 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.

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

### 7.2.3 Clean MAC address table

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **mac address-table clean** | Clean MAC address table. |

### 7.2.4 Configure maximum learnt MAC enties of port

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface** *{interface_type slot/port}* | Enter interface configuration mode. |
| **Step 3** | **mac-address mac-limit**<*0-16384*> | 0 means no limitation. |
| **Step 4** | **exit** | 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.

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

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **show mac address-table agingtime** | Show MAC address aging time. |

# 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.

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **monitorsession***session_number***destinationinterface***interface_typeinterface_num* | Confire mirroring destination port.<br>Session number is 1~4. |
| **Step 3** | **show monitor session all** | Show mirroring configurations. |
| **Step 4** | **write** | 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.

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **monitor session***session_number***sourceinterface***interface_typestart_interface_num* [ **-** *end_interface_num***]** {**both**\|**rx**\|**tx**} | Configure mirroring source port.<br>session_number is 1-4.<br>**Both** means received data and transmitted data.<br>**rx**means received data.<br>**tx** means transmitted data. |
| **Step 3** | **show monitor session all** | Show mirroring configurations. |
| **Step 4** | **write** | Save configurations. |

## 8.3 Delete port mirroring

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **no monitor session** *session_number*{**[destination \| source] interface***interface_typeslot/port*} | Delete port mirroring. session_number is 1-4 |
| **Step 3** | **show monitor session all** | Showmirroring 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2a** | **ip igmpsnooping enable** | Enable IGMP Snooping. |
| **Step 2b** | **no ip igmp snooping** | Disable IGMP snooping. |
| **Step 3** | **show ip igmpsnooping configuration** | Show IGMP snooping configurations. |
| **Step 4** | **write** | 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **ip igmp snooping forward vlan** *vlan-id* **mode { flood ｜ forward ｜ strict-forward}** | Configure multicast data forwarding mode. |
| **Step 3** | **write** | 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface***{interface_type slot/port}* | Enter interface configuration mode. |

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

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

### 9.1.5 Configure static multicast

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

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

### 9.1.6 Configure fast leave

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

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

### 9.1.7 Configure multicast group limit

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

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

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

| | | |
|---|---|---|
| | > | |
| **Step 2c** | **ip igmp snoopinglastmember-queryresponse**<*1-255*> | Configure specific query response time. Default is 1s. |
| **Step 3** | **show ip igmpsnooping configuration** | Show IGMP configurations. |
| **Step 4** | **write** | 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2a** | **ip igmp snooping general-query-packet**<*enable*\|*disable*> | Enable or disable general query function. Default is disable. |
| **Step 2b** | **ip igmp snooping general-query-time**<*10-255*> | Configure general query interval. Default is 126s. |
| **Step 3** | **show ip igmpsnooping configuration** | Show IGMP configurations. |
| **Step 4** | **write** | 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **ip igmp snooping member-query source-ip**<*A.B.C.D*> | Configure source IP of query message. Default is 1.1.1.1. |
| **Step 3** | **show ip igmpsnooping configuration** | Show IGMP configurations. |
| **Step 4** | **write** | 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 muticast member aging time as the following table shows.

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |

| | | |
|---|---|---|
| **Step 2** | **ip igmpsnooping host-aging-time***value* | Configure multicast port member aging time.<br>Value range is 10-3600s, defaultis260s. |
| **Step 3** | **show ip igmpsnooping configuration** | Show IGMP configurations. |
| **Step 4** | **write** | Save configurations. |

### 9.1.12 Show multicast gourp information

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

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

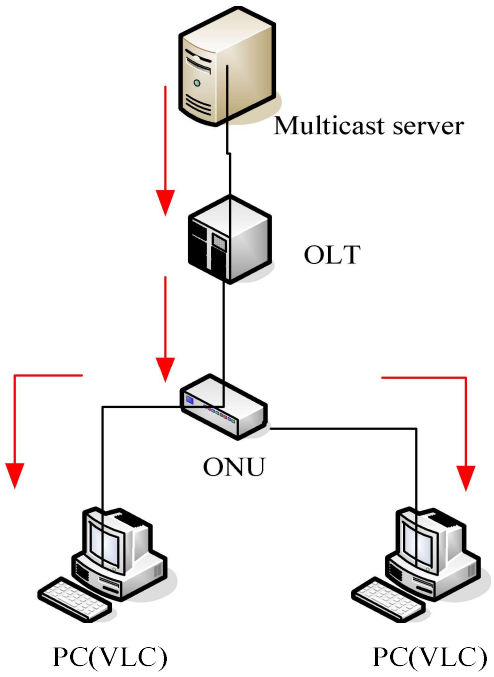
multicast is VLAN 100.

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.
- ACLbased 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 |
| ACLbased on MAC address | 2000-2999 | 1000 |
| ACL based on port binding | 5000-5999 | 1000 |
| ACL based on QoS | 6000-6999 | 1000 |

## 10.2 ACL confiuration

ACL configuration mainly includes:

- IP Standard ACL.
- IP Extended ACL.
- ACLbased 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** | **configure terminal** | Enter global configuration mode. |

| | | |
|---|---|---|
| **Step 2** | **access-list** *access-list-number* | Enter ACL configuration mode. *access-list-number* is ACL index.range:0-999. |
| **Step 3** | **subset ip (permit\|deny)**<*A.B.C.D*>[*net-mask*]<br>**subset ip (permit\|deny) host** <*A.B.C.D*><br>**subset ip [permit\|deny] any** | Configure ACL rule.<br><A.B.C.D>: define based on source IP address and mask ACL rule.<br>**Host**: define based on single IP address ACL rule.<br>**Any**: define based on any source IP address ACL rule. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show access-list[***access-list-number* \| **all]** | Show ACL configurations. |
| **Step 6** | **write** | 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** | **configure terminal** | Enter global configration mode. |
| **Step 2** | **access-list** *access-list-number* | Enter ACL configuration mode. *access-list-number* is ACL index. range:1000-1999. |
| **Step 3** | **subset protocol** {**deny**\| **permit**} *protocol*{ <*A.B.C.D*> *net-mask* {<*A.B.C.D*> *net-mask*\|**host** <*A.B.C.D*>\| **any**}[**match** {**dscp** *priority*\|**precedence***priority* \| **tos** *priority*}][**set** {**dscp***priority*\| **precedence** *priority* \| **tos***priority*}] | Configure IP extended ACL rule. Parameter *protocol* should be icmp, igmp, igrp, ip, ospf, pim, tcp, or udp, etc. it also can be replaced by protocol code 0~255. |
| **Step 4** | **exit** | Exit global configuration mode. |
| **Step 5** | **show access-list[***access-list-number* \| **all** ] | Show ACL configurations. |
| **Step 6** | **write** | 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** | **configure terminal** | Enter global configuration mode. |

| | | |
|---|---|---|
| **Step 2** | **access-list** *access-list-number* | Enter ACL configuration mode. *access-list-number* is ACL index. range:2000-2999. |
| **Step 3** | **subset ethernet** [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. |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show access-list[***access-list-number* \| **all]** | Show ACL configurations. |
| **Step 6** | **write** | 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.

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

| | | |
|---|---|---|
| **Step 6** | **write** | Save configurations. |

### 10.2.5 ACL based on QoS

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

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter globle configuration mode. |
| **Step 2** | **interface** *{interface_type slot/port}* | Enter interface configuration mode. |
| **Step 3a** | **ip access-group***access-list-number* **in** | Apply ACL rule to port. |

| | | |
|---|---|---|
| **Step 3b** | **no ip access-group***access-list-number* **in** | Delete ACL rule from port. |
| **Step 4** | **exit** | Exit to glogbal configuration mode. |
| **Step 5** | **show access-list***access-list-number* | Show ACL configurations. |
| **Step 6** | **write** | 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)Permitspecific 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.

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

## 11.2 Configure queue mapping

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |

| | | |
|---|---|---|
| **Step 2** | **queue-scheduler tc** *priority* **queue** *queue* | Configure mapping relation between queues and priority. By default, priority 0~7 maps to queue 0~7 respectively. |
| **Step 3** | **show queue-scheduler priority mapping** | Show queue mapping. |
| **Step 4** | **write** | 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<br>Gigabit Ethernet :4<br>Fast Ethernet :19<br>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** | **configure terminal** | Enter global configuration mode. |
| **Step 2a** | **spanning-tree on** | Enable device's STP function.<br>By default, STP function is disabled. |

| | | |
|---|---|---|
| **Step 2b** | **no spanning-tree** | Disable device's STP function. |
| **Step 3** | **show spanning-tree** | Show STP configurations. |
| **Step 4** | **write** | 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.

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **spanning-tree mode [rstp \| stp]** | Configure spanning tree mode. It runs RSTP by default. |
| **Step 3** | **show spanning-tree** | Show STP configurations. |
| **Step 4** | **write** | 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 prority as the following table shows.

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **spanning-tree priority** *bridge-priority* | Configure device's bridge priority.<br>Priority range is 0~65535, default is 32768. |
| **Step 3** | **show spanning-tree** | Show STP configurations. |
| **Step 4** | **write** | 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **spanning-tree forward-time** *seconds* | Configure device's forward delay.<br>bridge-priority range is 4~30, default is 15. |
| **Step 3** | **show spanning-tree** | Show STP configurations. |
| **Step 4** | **write** | 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 ×(forward-delay －1) >= maximum-agemaximum-age >= 2 ×(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.

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter globalconfiguration mode. |
| **Step 2** | **spanning-tree hellotime***seconds* | Configure device's hello time. Hello time range is 1~10, default is 2. |
| **Step 3** | **show spanning-tree** | Show STP configurations. |
| **Step 4** | **write** | Save configurations. |

### 12.2.7 Configure max age time

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

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

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

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |

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

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

### 12.2.10Configure edge port

The port which connects with terminal host is EdgePort. In process of spanning tree recomputation, edge port can transfer to forwarding status derectly 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.

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |

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

### 12.2.11Configure 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.

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

## 12.3 Show STP information

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

| **Command** | **Function** |
|---|---|
| **show spanning-tree** | Show STP configurations and |

| | |
|---|---|
| | running status. |
| **show spanning-tree interface***{interface_type slot/port}* | Show STP configurations and running status of a port. |

# 13.OLT Management Configuration

## 13.1 Configure outband management

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

### 13.1.3 Show AUX port information

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

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **config terminal** | Enter global configuration mode. |
| **Step 2** | **gateway** <*A.B.C.D*> | Configure management gateway. **The gateway must be the same network segment with outband or inband management IP.** |
| **Step 3** | **no gateway** | Delete management gateway. |

| | | |
|---|---|---|
| **Step 4** | **show gateway** | Show management gateway configuration. |
| **Step 5** | **write** | 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.

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

## 14.2 ARP Proxy

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

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

| | | |
|---|---|---|
| | | mode. |
| **Step 5** | **write** | Save configurations. |

## 14.3 Static Route

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2a** | **ip route** *A.B.C.D A.B.C.D A.B.C.D* | Add static route rule. |
| **Step 2b** | **ip route***A.B.C.D/M A.B.C.D* | Add static route rule. |
| **Step 3a** | **no ip route***A.B.C.D A.B.C.D A.B.C.D* | Delete static route rule. |
| **Setp 3b** | **no ip route***A.B.C.D/M A.B.C.D* | Delete static route rule. |
| **Step 4** | **show ip route** | 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:

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **router rip** | Enable a RIP routing process, and enter router configuration mode. |
| **Step 3** | **network***ip-address/masklen* | 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. |
| **Step 4** | **neighbor***ip-address* | (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. |
| **Step 5** | **offset-list**(*access-list number*| *name*) **(in**|**out) metric**<*0-16*>**vlan**<*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. |
| **Step 6** | **timers basic***update timeout garbage* | (Optional) Adjust routing protocol timers. Valid ranges for all timers are 0 to 4294967295 seconds.<br>•update—Time between sending routing updates. The default is 30 seconds.<br>•invalid—Time after which a route is declared invalid. The default is 180 seconds.<br>•holddown—Time before a route is removed from the routing table. The default is 180 seconds.<br>•flush—Amount of time for which routing updates are postponed. The default is 240 seconds. |
| **Step 7** | **version**(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.<br>You can also use the interface commands ip rip {send \| receive} version 1 \| 2 \| 1 2} to control what versions are used for sending and receiving on |

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

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

| | | |
|---|---|---|
| **Step 5** | **exit** | Return to privileged EXEC mode. |
| **Step 6** | **show ip rip status** | Showing RIP current status. About the RIP timer, filter list,version,interface information. |
| **Step 7** | **show ip rip** | Showing RIP route information. |
| **Step 8** | **write** | 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:

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

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

### 14.4.4 Configuring RIP v1/2 Compatible

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interfacevlan***vlan_id* | Enter interface configuration mode, and specify the interface to configure. |
| **Step 3** | **ip rip receive version**（1\|2）（1\|2） | Configure receive v1 or v2 or v1 and v2. |
| **Step 4** | **ip rip send version**（1\|2）（1\|2） | Configure send v1 or v2 or v1 and v2. |
| **Step 5** | **exit** | Return to privileged EXEC mode. |
| **Step 6** | **show ip rip status** | Showing RIP current status. About the RIP timer, filter list,version,interface information. |
| **Step 7** | **show ip rip** | Showing RIP route information. |
| **Step 8** | **write** | 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **router ospf** | Enable OSPF routing, and enter router configuration mode. |
| **Step 3** | **router-id** *A.B.C.D* | (Optional)Configure router id. |
| **Step 4** | **network***A.B.C.D/M***area***(A.B.C.D\|<0-4294967295>)** | 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** | **exit** | Return to privileged EXEC mode. |
| **Step 6** | **write** | 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface vlan***vlan_id* | Enter interface configuration mode, and specify the Layer 3 interface to configure. |

| | | |
|---|---|---|
| **Step 3** | **ip ospf cost** <*1-65535*> | (Optional) Explicitly specify the cost of sending a packet on the interface. |
| **Step 4** | **ip ospf retransmit-interval** *seconds* | (Optional) Specify the number of seconds between link state advertisement transmissions. The range is 1 to 65535 seconds. The default is 5 seconds. |
| **Step 5** | **ip ospf transmit-delay***seconds* | (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. |
| **Step 6** | **ip ospf priority***number* | (Optional) Set priority to help determine the OSPF designated router for a network. The range is from 0 to 255. The default is 1. |
| **Step 7** | **ip ospf hello-interval***seconds* | (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. |
| **Step 8** | **ip ospf dead-interval***seconds* | (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. |
| **Step 9** | **ip ospf authentication-key***auth_key* | (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** | **ip ospf message-digest-key***keyid* **md5***key* | (Optional) Enable MDS authentication.<br>•keyid—An identifier from 1 to 255.<br>•key—An alphanumeric password of up to 16 bytes. |
| **Step 11** | **ip ospf authentication** | Enable ospf authentication. |
| **Step 12** | **ip ospf authentication message-digest** | Enable ospf MD5 authentication. |
| **Step 13** | **exit** | Return to privileged EXEC mode. |
| **Step 14** | **show ip ospf interface***[interface-name]* | Display OSPF-related interface information. |
| **Step 15** | **write** | 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:

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **router ospf** | Enable OSPF routing, and enter router configuration mode. |
| **Step 3** | **area***area-id***authentication** | (Optional) Allow password-based protection |

| | | |
|---|---|---|
| | | against unauthorized access to the identified area. The identifier can be either a decimal value or an IP address. |
| **Step 4** | **area***area-id***authenticationmessage-digest** | (Optional) Enable MD5 authentication on the area. |
| **Step 5** | **area***area-id***stub***[no-summary]* | (Optional) Define an area as a stub area. The no-summary keyword prevents an ABR from sending summary link advertisements into the stub area. |
| **Step 6** | **area***area-id***nssa***[no-summary]* | (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:<br>•no-summary—Select to not send summary LSAs into the NSSA. |
| **Step 7** | **area***area-id***range***address/masklen* | (Optional) Specify an address range for which a single route is advertised. Use this command only with area border routers. |
| **Step 8** | **exit** | Return to privileged EXEC mode. |
| **Step 9** | **show running ip ospf** | Display OSPF running-config information. |
| **Step 10** | **show ip ospf database** | Display lists of information related to the OSPF database for a specific router. |
| **Step 11** | **write** | 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **router ospf** | Enable OSPF routing, and enter router configuration mode. |
| **Step 3** | **area***area-id***virtual-link***A.B.C.D** | (Optional) Establish a virtual link and set its parameters. |
| **Step 4** | **default-information originate {[always]}*1 {[metric]** *<0-16777214>***}*1 {[metric-type]** *(1\|2)}****1 {[route-map]** *<WORD>***}*1** | (Optional) Force the ASBR to generate a default route into the OSPF routing domain. Parameters are all optional. |
| **Step 5** | **distance ospf {[inter-area** *dist1***] [inter-area** *dist2***] [external** *dist3***]}** | (Optional) Change the OSPF distance values. The default distance for each type of route is 110. The range is 1 to 255. |
| **Step 8** | **exit** | Return to privileged EXEC mode. |
| **Step 9** | **show running ip ospf** | Display OSPF running-config information. |
| **Step 10** | **show ip ospf database** | Display lists of information related to the OSPF database for a specific router. |

| | | |
|---|---|---|
| **Step 11** | **write** | Save configurations. |

## 14.5.5 Monitoring OSPF

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

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **show ip ospf database** *[router] [self-originate]*<br>**show ip ospf database***[router] [adv-router [ip-address]]*<br>**show ip ospf database** *[network] [self-originate]*<br>**show ip ospf database***[network] [adv-router [ip-address]]*<br>**show ip ospf database***[summary] [self-originate]*<br>**show ip ospf database***[summary] [adv-router [ip-address]]*<br>**show ip ospf database***[asbr-summary] [self-originate]*<br>**show ip ospf database***[asbr-summary] [adv-router [ip-address]]*<br>**show ip ospf database***[external] [self-originate]*<br>**show ip ospf database***[external] [adv-router [ip-address]]* | Display lists of information related to the OSPF database. |
| **Step 3** | **show ip ospf route** | Display lists of information related to the OSPF route. |
| **Step 4** | **show ip ospf interface***[interface-name]* | Display OSPF-related interface information. |
| **Step 5** | **show ip ospf neighbor** | 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2a** | **ip access-list** *access_list_index* **{permit\|deny}** <*A.B.C.D*> <*wildcard_mask*><br><br>**ip access-list** *access_list_index* **{permit\|deny} host** <*A.B.C.D*><br><br>**ip access-list** *access_list_index* **{permit\|deny} any** | Define a standard access-list, access_list_index ranges from 1-99 to 1300-1999,<br>< A.B.C.D. > < wildcard_mask > defines standard IP access based on the source IP address or mask;<br>Host defines standard IP access based on a single source IP address;<br>Any standard IP access based on any source IP address; |
| **Step 2b** | **ip access-list** *access_list_index* **{permit\|deny}** <*A.B.C.D*> <*wildcard_mask*> {<*A.B.C.D*> < *wildcard_mask*> \| **host** <*A.B.C.D*> \| **any**}<br><br>**ip access-list** *access_list_index* **{permit\|deny} host** <*A.B.C.D*> {<*A.B.C.D*> <*wildcard_mask*> \| **host** <*A.B.C.D*> \| **any**}<br><br>**ip access-list** *access_list_index* | Define an extended access-list, access_list_index ranges from 100-199 to 2000-2699,<br>< A.B.C.D. > < wildcard_mask > defines extended IP access based on the source IP address or mask;<br>Host defines extended IP access based on a single source IP address;<br>Any extended IP access based on |

| | | |
|---|---|---|
| | **{permit\|deny} any** {<*A.B.C.D*> <*wildcard_mask*> \| **host** <*A.B.C.D*> \| **any**} | any source IP address; |
| | **no ip access-list** *access_list_index* | Delete access-list |
| **Step 3** | **exit** | Return to privileged EXEC mode. |
| **Step 4** | **show ip access-list** | Show access-list information |
| **Step 5** | **write** | 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.

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

| | | |
|---|---|---|
| | | of prefix lengths to match, and the specified ge values and values must satisfy:<br>Prefix_len < ge_value < le_value < 32. |
| **Step 2b** | **no ip prefix-list** *prefix_list_name* | Delete prefix-list |
| **Step 3** | **exit** | Return to privileged EXEC mode. |
| **Step 4** | **show ip prefix-list [detail \| summary]** | Show ip prefix-list information. |
| **Step 5** | **write** | 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 0.0.0.0.0.0/0 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 autonomic 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

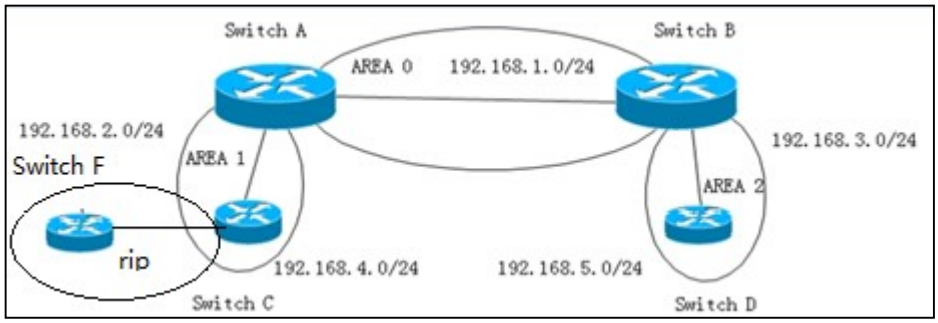
| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **router rip** | Start RIP and enter RIP configuration mode |
| **Step 3** | **distance** <*1-255*> | Set the administrative distance, default is 120. |
| **Step 4** | **default-metric** <*1-16*> | Default measurement |
| **Step 5** | **redistribute** *(kernel\|connected\|static\|ospf)* **{metric** <*0-16*>**}*1 {route-map** <*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** | **passive-interface** *<IFNAME> {A.B.C.D}*1* | Configure the passive interface |
| **Step 7** | **offset-list** *(<access-list>) (in\|out) <0-16>* **{vlan** *<1-4094>***}*1** | Used to adjust measurements |
| **Step 8** | **show running-config** | Show running-config information |

## 14.6.2.2 OSPF Route Redistribution

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

For example：



| Configuration | Result |
|---|---|
| switch c:<br>router ospf<br>router-id 3.3.3.3<br>network 192.168.2.3/24 area 1<br>redistribute connected metric 30(10)<br>redistribute rip metric 30(10) | When configured with metric of 30 on switch c，<br>On switch a：O E2 192.168.4.0/24 [110/30] via 192.168.2.3, 01:01:27,Vlan2<br>When configured with metric of 10 on switch c，<br>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 **istribute-list in** command filters routing selection updates coming in from the specified interface.

## 14.6.3.1 Distance Vector Routing Protocol RIP

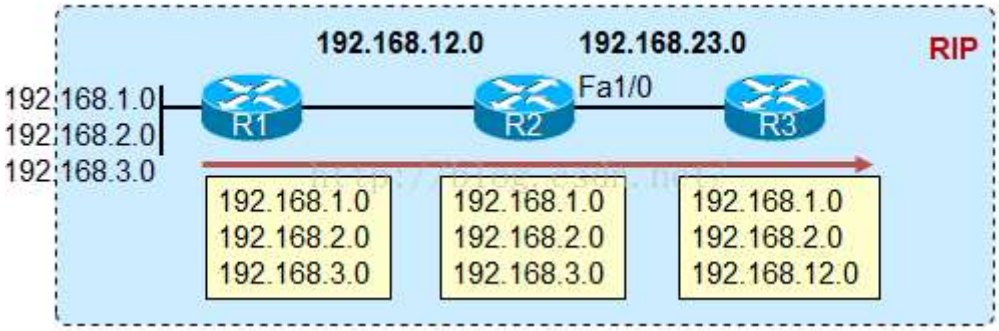
Routing information is passed between routers, and the distribution list has absolute control over routing information.So if it is in the direction, then through the deployment of distribution list, can filter the particular route, the executive distribution lists local routing routing table changes, 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** | **configure terminal** | Enter global configuration mode.. |
| **Step 2** | **router rip** | Start RIP and enter RIP configuration mode |
| **Step 3** | **distribute-list** <*access-list*> **(in\|out) {<ifname>}*1** | Filter routing using the access control list |
| **Step 4** | **distribute-list prefix** <*prefix-list*> **(in\|out)** {<*WORD*>}***1** | Filter routing using prefix lists |
| **Step 5** | **show running-config** | 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

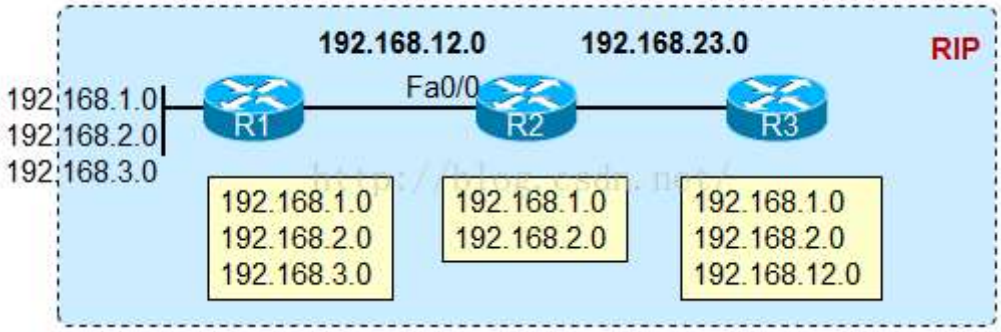
R2(config)# access-list 1 permit any

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.

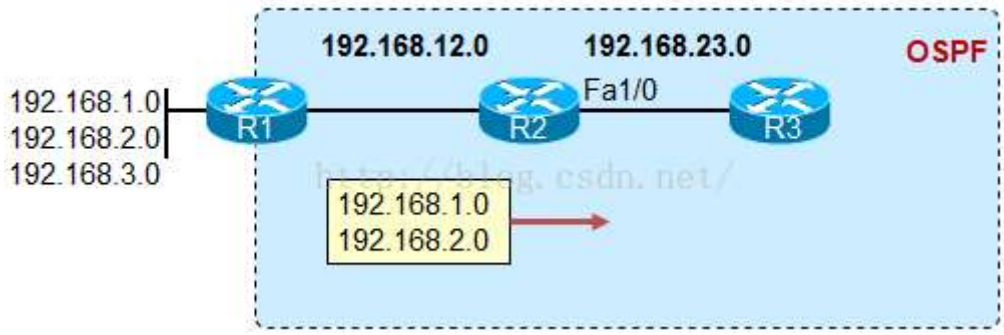
**Out direction,** the distribution list can only work on the ASBR that performs the routing reissue action, and only works for externally introduced routes.Because when performing redistribute, OSPF actually these exterior routing is introduced in the form of routing in, so the distribution list can 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:

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode.. |
| **Step 2** | **router ospf** | Start ospf and enter ospf configuration mode |
| **Step 3** | **distribute-list** <*access-list*> **out (kernel\|connected\|static\|rip)** | Use the access control list for redistribution |
| **Step 5** | **show running-config** | 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)

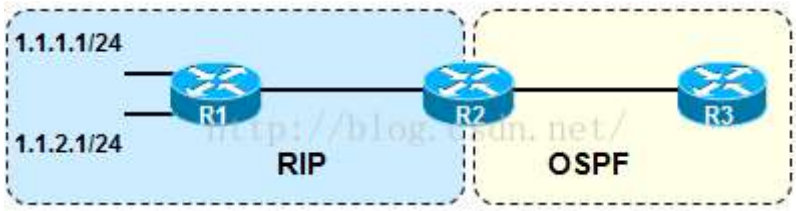
R1 (config - the router) # redistribute connected subnets

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

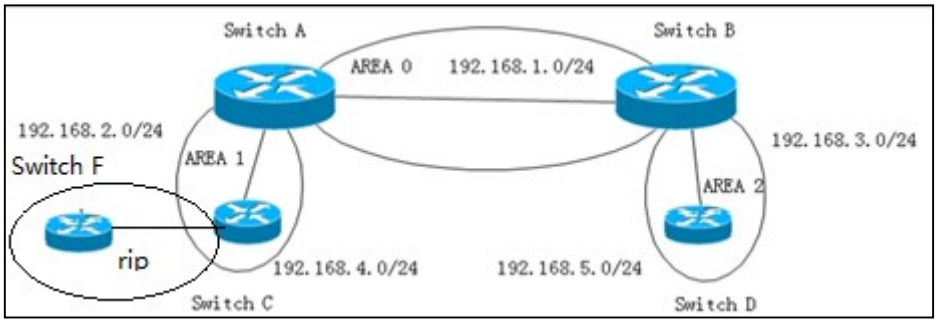
Redistribute rip metric 10 subnets

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 |
|---|---|

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

### 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.

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **route-map** *map_name* **[permit\|deny]** | Configure a route-map and |

| | | |
|---|---|---|
| | *sequence_number* | enter the route-map configuration mode. |
| **Step 3** | **match ip address** *access_list_number* | Matching the specified access-list, the range of access_list_number 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** | **match ip address prefix-list** *prefix_list_name* | Match the specified prefix-list. |
| **Step 5** | **match ip next-hop** *access_list_number* | Matching the next hop routing address through the specified access-list, the access_list_number 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** | **match ip next-hop prefix-list** *prefix_list_name* | Match the next hop routing address through the specified prefix-list. |
| **Step 7** | **match interface** *interface_name* | Matches the routing of the next outgoing interface that is one of the specified interfaces |
| **Step 8** | **match metric** *metric_value* | Matching the specified routing metrics, metric_value ranges from 0-4294967295. |
| **Step 9** | **match tag** *tag_value* | Matches the specified routing tag, and the tag_value range is 1-4294967295. |
| **Step 10** | **set metric** *metric_value* | Set the metrics for the reroute routing, and metric_value ranges from 0-4294967295. |
| **Step 11** | **set metric-type** *metric_type* | Sets the measurement value type for the redistributed routing. |
| **Step 12** | **set tag** *tag_value* | Sets the tag for the redistributed routing. |
| **Step 13** | **set ip next-hop** *metric_value* | Specifies the measure of the |

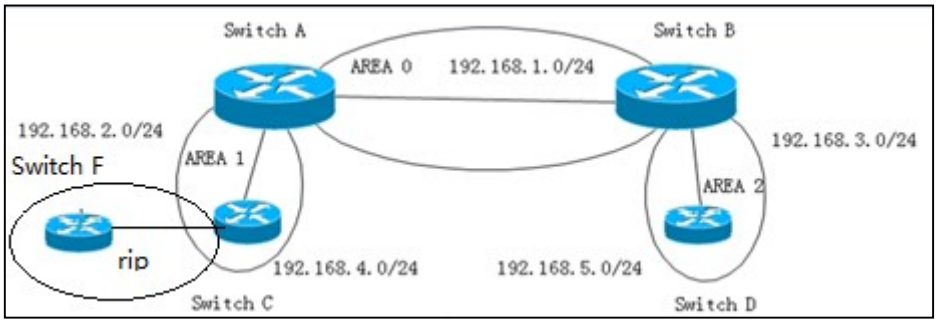
| | | |
|---|---|---|
| | | next hop of forwarding. |
| **Step 14** | **exit** | Return to privileged EXEC mode. |
| **Step 15** | **show route-map** | Show route-map information |
| **Step 16** | **write** | Save configurations. |

To delete a route-map entry, use the **no route-map** *map_name* command.Delete the match entry and use the **no match** command.Delete a set entry, using the **no set** command.

## 14.6.4.2 Link Status Routing Protocol OSPF

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **router ospf** | Start ospf and enter ospf configuration mode |
| **Step 3** | **redistribute** (kernel\|connected\|ospf\|static) {metric <0-16777214>} {metric-type (1\|2)} {route-map <WORD>} | Redistribute direct connection, kernel, ospf protocol, static routing information to rip protocol.Get the ospf protocol out there. |
| **Step 5** | **show running-config** | Show running-config information |

For example




| Configuration | Result |
|---|---|
| switch c:<br>ip access-list 1 permit 192.168.6.0 0.0.0.255<br>ip access-list 2 permit 192.168.7.0 0.0.0.255<br>ip prefix-list 1 seq 5 permit 192.168.6.0/24<br>ip prefix-list 2 seq 5 permit 192.168.7.0/24 | 1）switch c execute：redistribute rip route-map test1<br>switch b result<br>========== OSPF external routing table ========== |

| | |
|---|---|
| route-map test1 permit 10<br>match ip address 1<br>set metric 300<br>set metric-type type-1<br>!<br>route-map test1 permit 30<br>match ip address 2<br>set metric 500<br>!<br>route-map test2 permit 20<br>match ip address 2<br>set metric 500<br>!<br>route-map test3 permit 40<br>match ip address prefix-list 1<br>set metric 400<br>!<br>route-map test3 permit 50<br>match ip address prefix-list 2<br>set metric 600<br>! | N E1 192.168.6.0/24 [302] tag: 0<br>via<br>192.168.1.1, ethv0.1<br>N E2 192.168.7.0/24 [2/500] tag: 0<br>via<br>192.168.1.1, ethv0.1<br>2）switch c execute：redistribute rip route-map test2<br>switch b result<br>N E2 192.168.7.0/24 [2/500] tag: 0<br>via<br>192.168.1.1, ethv0.1<br>3）switch c execute：redistribute rip route-map test3<br>switch b result<br>N E2 192.168.6.0/24 [2/400] tag: 0<br>via<br>192.168.1.1, ethv0.1<br>N E2 192.168.7.0/24 [2/600] tag: 0<br>via<br>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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **router ospf** | Enter the OSPF configuration mode. |
| **Step 3** | **area** *area-id* **filter-list prefix** <*prefix*> *(in\|out)* | Configure the list of prefixes within the region. |
| **Step 4** | **exit** | 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 .DHP (Dynamic Host configuration Protocol) is created to solve this problem .It concludes DHCP Server and DHCP Client.Requested by client, IP address are allocated by the server.Configure DHCP Server as the following table show:

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

1.Single DHCP relay configuration：

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

2.、 Multiple DHCP relay configuration：

| | Command | Function |
|---|---|---|
| **Step 1** | **config terminal** | Enter global configuration mode. |
| **Step 2** | **dhcp-server group<groupname>** | Add a DHCP server group，and enter group configuration mode. |
| **Step 3a** | **dhcp-server A.B.C.D** | Add the DHCP server to the group. |
| **Step 3b** | **no dhcp-server A.B.C.D** | Delete DHCP server |
| **Step 4** | **exit** | Exit to the global configuration mode |
| **Step 5** | **interface vlan** *vlan_id* | Add a VLAN and enter to VLAN interface configuration *vlan_id(*1－4094)； |
| **Step 6a** | **dhcp relay server-select<groupname>** | Select DHCP server group 。 |
| **Step 6b** | **no dhcp relay server-select<groupname>** | Delete the DHCP server group。 |
| **Step 7** | **exit** | Exit to global configuration mode |
| **Step 8** | **show dhcp-relay configure** | Sow DHCP relay configuration. |
| **Step 9** | **copy running-config startup-config** | 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** | **config terminal** | Enter global configuration mode. |
| **Step 2** | **dhcp-snooping （enable\|disable）** | Enable/disable DHCP Snoopin.（DHCP Snooping enable，can not open dhcp server and dhcp relay） |
| **Step 3a** | **dhcp-snooping vlan <1-4095>…** | Configure DHCP Snooping vlan list |
| **Step3b** | **nodhcp-snooping vlan <1-4095>…** | Delete DHCP Snooping vlan list |
| **Step 4** | **exit** | Exit to global configuration mode. |
| **Step 5** | **show dhcp-snooping configuration** | Show DHCP Snooping configuration。 |
| **Step 6** | **copy running-config startup-config** | Save configuration. |

B.Configure DHCP Snooping option82

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

C.Configure DHCP Snooping binding list

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **config terminal** | Enter global configuration mode. |

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

D.Configure DHCP Snooping port

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

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

# 16.PON Management Configuration

## 16.1Enable/Disable PON

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

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

## 16.2PON 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3a** | **pon encryption triple-churningkey_timer** *<774-786426>* | Enable PON downstream encryption. |
| **Step 3b** | **no pon encryption** | Disable PON downstream encryption. |
| **Step 4** | **show pon encryption** | Show pon encryption configuration. |

## 16.3Configure 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 no 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 adopt 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.

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

## 16.4 PON ONU laser detect

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

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

## 16.5 Show PON port statistics

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

| **Command** | **Function** |
|---|---|

| | | |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **show pon statistics** | Show PON port statistics. |

## 16.6 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.

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **show pon optical transceiver** | Show pon optical parameters. |

# 17.ONU Management Configuration

## 17.1 ONU basic configuration

### 17.1.1 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **onu auth-mode {disable\|mac\|loid\|hybrid}** | Configure ONU authentication mode. |
| **Step 4** | **show onu auth-mode** | Show ONU authentication mode. |
| **Step 5** | **show onu auth-info** | Show authenticated ONU. |
| **Step 6** | **show onu auto-find** | Show registered but not authenticated ONU. |

### 17.1.2 Remove authorized ONU

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |

| | | |
|---|---|---|
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **no onuauth onuid**<*onuid*> | Remove authorized ONU. |

### 17.1.3 Deregister or reset ONU

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

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

### 17.1.4 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3a** | **onu mac-auth {add\|del}**<*xx:xx:xx:xx:xx:xx*> | Add or delete MAC white list. |
| **Step 3b** | **onu black-mac-auth {add\|del}**<*xx:xx:xx:xx:xx:xx*> | Add or delete MAC black list. |
| **Step 3c** | **onu {mac-auth\| black-mac-auth} clean** | Clean MAC white list or black list. |
| **Step 4** | **show onu mac-auth** | Show ONU MAC white list. |
| **Step 5** | **show onu black-mac-auth** | Show ONU MAC black list. |

### 17.1.5 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **onu loid-auth** | Add or delete LOID list. |

| | | |
|---|---|---|
| | **{add\|del}**<*loid*>[<*password*>]*1 | |
| **Step 4** | **onu loid-auth clean** | Clean LOID list. |
| **Step 5** | **show onu loid-auth** | Show onu LOID list. |

### 17.1.6 Measure ONU distance

Use the following commands to measure authorized ONU distance.

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **show onu**<*onuid*>**rtt** | Measure ONU distance. |

### 17.1.7 Configure ONU description string

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interfaceconfiguration mode. |
| **Step 3** | **onu**<*onuid*>**description**<*string*> | Add description string to ONU. |
| **Step 4** | **show onu**<*onuid*>**description** | Show ONU description. |

### 17.1.8 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.

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **onu**<*onuid*>**encryption{enable\|disable}** | Enable/Disable ONU downstream encryption. |
| **Step 4** | **show onu**<*onuid*>**encryption** | Show onu downstream encryption. |

### 17.1.9 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3a** | **onu** <*onuid*> **upstream fir** <*0-950000*> **cir** <*1-950000*> **pir** <*512-1000000*> **weight** <*1-20*> | 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** | **no onu** <*onuid*> **upstream** | Delete ONU upstream bandwidth configuration. |
| **Step 4** | **show onu** <*onuid*> **upstream** | Show onu upstream bandwidth. |

### 17.1.10Configure 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3a** | **onu** <*onuid*> **downstream pir** <*0-1000000*> **weight** <*1-16*> | Configure ONU downstream bandwidth. |
| **Step 3b** | **no onu** <*onuid*> **downstream** | Delete ONU downstream bandwidth configuration. |
| **Step 4** | **show onu** <*onuid*> **downstream** | Show onu downstream bandwidth. |

### 17.1.11Configure ONU MAC limit

Limite the ONU MAC address

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter globalconfiguration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **onu**<1-65535>[mac-limit] <0-16383> | Set the onu mac limit |
| **Step 4** | **Show onu** <1-65535>[mac-limit] | Show the MAC limit count |

### 17.1.12Show ONU status

Can show the time of onu register, deregister and running

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter globalconfiguration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **show onustatus** <all> | Show ONU status |

### 17.1.13Show ONU statistics

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

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter globalconfiguration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **show onu**< *1-65535*>**statistics** | Show ONU statistics. |

## 17.2 ONU global configuration

### 17.2.1 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 |
|---|---|
| **show onu**< *onuid*>**ctc onu_info** | Display ONU basic information. |
| **show onu**< *onuid*>**ctc ctc_info** | Display CTC OAM version which ONU supports. |
| **show onu**<*onuid*>**ctconu_sn** | Display ONU vendor ID, version and PON MAC. |
| **show onu**<*onuid*>**ctcfw_ver** | Display PON firmware version. |
| **show onu**<*onuid*> **ctc chip_id** | Display PON chipset model. |
| **show onu**<*onuid*>**ctc cap_1** | 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. |
| **show onu**<*onuid*>**ctc opm_diag** | Display ONU optical transceiver main parameters and diagnosis. |
| **showonu**<*onuid*>**ctc cap_2** | Display ONU main specifications; include multi LLID, protection type, slot number, port type and number, backup battery. |
| **showonu**<*onuid*>**ctc cap_3** | Display ONU IPv6 capability and transceiver power force shutdown. |
| **show onu** <*onuid*>**ctc fast_leave_ability** | Display ONU multicast fast leave capability. |
| **show onu** <*onuid*> **ctc fec_ability** | Display ONU FEC capability. |
| **show onu** <*onuid*>**ctc power_saving_cap** | Display ONU enegy-saving capability and wake up mechanism. |

### 17.2.2 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **upgrade onu image** <*filename*><*A.B.C.D*> | Configure ONU firmware name and TFTP server. |
| **Step 3** | **upgrade onu select pon** <*pon_num*> *{*<*onuid_list*>*}*8* | Select ONU. ONU ID format is 1-2. |
| **Step 4** | **upgrade onu start** | 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**.

### 17.2.3 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** |
|---|---|

| | | |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **auto-upgrade**<*force*><*onu*>***vendor*** <*string*>***model***<*string*>***swversion***<*string*> ***image***<*filename*><*A.B.C.D*> | Configure ONU firmware verdor id ,model id, swversion,file name and TFTP server. |

**Notice:**

1.When the ONU come online, the OLT will upgeade 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*>

### 17.2.4 Configure ONU management IP

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **onu** <*onuid*> **ctc 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* | Configure ONU management IP. |
| **Step 4** | **show onu**<*onuid*>**ctc mgmt** | Show ONU management IP. |

### 17.2.5 Configure ONU SNMP

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **onu** <*onuid*> **ctcmdu_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 | Configure MDU SNMP parameters. |
| **Step 4** | **show onu**<*onuid*>**ctc mdu_snmp** | Show MDU SNMP |

| | |
|---|---|
| | configurations. |

### 17.2.6 Confiure ONU multi LLID

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

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

### 17.2.7 Configure ONU primary PON interface

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter globalconfiguration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **onu**<*onuid*> **ctc active_pon**<*0-8*> | Configure ONU primary PON interface. |
| **Step 4** | **show onu**<*onuid*> **ctc active_pon** | Show ONU primary PON interface. |

### 17.2.8 Configure ONU FEC function

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **onu** <*onuid*>**ctc fec_mode {enable\|disable}** | Enable/Disable ONU FEC function. |
| **Step 4** | **show onu**<*onuid*>**ctc fec_mode** | Show ONU FEC function configuration. |

### 17.2.9 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** | **configure terminal** | Enter global configurationmode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **onu**<*onuid*> **ctc holdover**<*0-65535*> | Configure optical link protection. value 0 means protection is disabled. |
| **Step 4** | **show onu**<*onuid*>**ctc holdover** | Show onu optical link protection configuration. |

### 17.2.10Configure ONU SLA function

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **onu** <onuid> **ctc sladisable** | Disable ONU SLA function. |
| **Step 4a** | **onu** <*onuid*> **ctcslaenablesp_basic** | Enable ONU SLA function. |
| **Step 4b** | **onu** <*onuid*> **ctc sla enable {wrr\|sp_wrr} {queue** <*1-8*> **fix_packet_size** <*0-1900*>**fix_bandwith**<*0-1024*> **guaranteed-bandwidth**<*1-1024*> **best_effort_bandwith**<*1-1024*> **weight** <*0-100*>**}***8* | Enable SLA function and configure weight of each queue. |
| **Step 5** | **show onu** <*onuid*>**ctcsla** | Show ONU SLA configurations. |

### 17.2.11Configure ONU multicast mode

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |

| | | |
|---|---|---|
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **onu** <*onuid*> **ctcmc_switch {snooping\|control}** | Snooping: enable IGMP/MLD Snooping protocol for multicast member management.<br>Control: enable CTC controllable multicast protocol for member management. |
| **Step 4** | **show onu**<*onuid*>**ctc mc_switch** | Show ONU multicast mode configuration. |

### 17.2.12Configure ONU fast leave function

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **onu**<*onuid*>**ctc fast_leave** {**enable\|disable**} | Enable or disable ONU fast leave function. |
| **Step 4** | **show onu**<*onuid*>**ctc fast_leave** | Show onu fast leave configuration. |

### 17.2.13Restart ONU

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **onu**<*onuid*>**ctc reset** | Restart ONU. |

### 17.2.14Configure ONU power saving mode

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter gloable configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface |

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

### 17.2.15Configure 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.

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

### 17.2.16Configure ONU optical link protection mechanism

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter globalconfiguration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface |

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

### 17.2.17Confiure ONU PON power supply control

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

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

### 17.2.18Configure ONU MAC aging time

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |

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

### 17.2.19Configure 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.

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

### 17.2.20Clear/show ONU PON port statistics

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

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

## 17.3 ONU port configuration

### 17.3.1 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.

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

### 17.3.2 Enable/Disable ONU port

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

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

### 17.3.3 Configure ONU port autonegotiation

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

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

### 17.3.4 Configure ONU port re-autonegotiation

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

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

### 17.3.5 Configure ONU port upstream policy

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

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

### 17.3.6 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **onu**<*onuid*>**ctc eth**<*port-num*>**rate_limit cir**<1-1048576> [**pir**] <1-1048576> | Configure ONU port downstream rate limit. |
| **Step 4** | **onu**<*onuid*>**ctc eth**<*port-num*>**rate_limit default** | Delete ONU port downstream rate limit. |
| **Step 5** | **show onu**<*onuid*>**ctc eth**<*port-num*>**rate_limit** | Show ONU port downstream policy configuration. |

### 17.3.7 Configure ONU port flow control

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

table shows.

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

### 17.3.8 Configure ONU port loopback detection

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

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

### 17.3.9 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **onu**<*onuid*>**ctc eth**<*port-num*>**loop**[**enable\|disable**] | Enable: when it detects a loopback, the port will shutdown.<br>Disable: when it detects a loopback, the port will not shutdown. |

### 17.3.10Configure 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.

| | Command | function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **onu**<*onuid*>**ctc eth**<*port-num*>**vlan mode** [**transparent**\|**tag**\|**translation**\|**aggregation**\|**trunk**] | Configure port VLAN mode. |

### 17.3.11Configure 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.

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **onu**<*onuid*>**ctc eth**<*port-num*>**vlan pvid**<*pvid*>**pri**<*pri*> | Pvid range: 1-4095<br>Pri range: 0-7. |

### 17.3.12Configure ONU port VLAN translation entries

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

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

### 17.3.13Configure ONU port VLAN trunk entries

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

| Command | Function |
|---|---|

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

### 17.3.14Configure ONU port VLAN aggregation entries

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

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

### 17.3.15Show ONU port VLAN configurations

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

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

### 17.3.16Configure 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.

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global |

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

### 17.3.17Configure ONU port multicast VLAN

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

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

### 17.3.18Configure 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3** | **onu**<*onuid*>**ctc eth** <*port-num*>**mc_maxgrp**<0-4096> | Configure ONU maximum multicast gourps. |
| **Step 4** | **showonu**<*onuid*>**ctc eth** <*port-num*>**mc_maxgrp** | Show ONU maximum multicast gourps. |

### 17.3.19Configure 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3a** | **onu** <*onuid*> **ctc eth** <*port-num*>**mc_tagstrip {enable\|disable}** | Enable: strip VLAN tag of multicast streams and query message.<br>Disable: don't strip VLAN tag of multicast streams and query message. |
| **Step 3b** | **onu** <*onuid*> **ctc eth** <*port-num*> **mc_tagstrip iptv set** {<*1-4095*> **to** <*1-4095*>}*8 | Modify multicast customer VLAN and query message VLAN to IPTV VLAN. |
| **Step 4** | **show onu** <*onuid*> **ctc eth** <*port-num*> **mc_tagstrip** | Show ONU port multicast VLAN stripconfigurations. |

### 17.3.20Configure ONU port statistics

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

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

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

### 17.3.21Clear/Show ONU port statistics

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

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

## 17.4 ONU remote voice configuration

### 17.4.1 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.

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

### 17.4.2 Configure global parameters

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

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

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

### 17.4.3 Enable/disable POTS port

Thesecommands are used toenable or disable POTS port.

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

### 17.4.4 Configure H.248protocol

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

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

| | | |
|---|---|---|
| | **h248_param_configheartbeat mode {disable\|h248} cycle** *<1-65535>* **count** *<1-65535>* | parameters. |
| **Step 5** | **onu** *<onuid>* **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 | Configure MGC and back up MGC informations. |
| **Step 6** | **show onu** *<onuid>* **ctc h248_param_config** | Show onu VoIP parameters of H.248 |

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

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

### 17.4.6 ConfigureRTP TID information(H.248)

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

### 17.4.7 Configure SIP protocol

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

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

### 17.4.8 ConfigureSIPaccountparameters of POTS

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

### 17.4.9 Configure fax mode

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter the pon interface configuration mode. |
| **Step 3** | **onu** *<onuid>* **ctcfax_modem_configvoice_t38 {enable\|disable} control {negotiation\|auto_vbd}** | Configure fax mode and the way of negotiation |

| | | |
|---|---|---|
| **Step 4** | **show onu** <*onuid*> **ctc fax_modem_config** | Show faxservice parameter information |

### 17.4.10VoIP module operation

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter the pon interface configuration mode. |
| **Step 3** | **onu** <*onuid*> **ctciad_oper {reregister\|deregister\|reset}** | Reregister: onu re-registration<br>Deregister: onu logout<br>Reset: reset VoIP module |

### 17.4.11ConfigureSIP digitmap

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

## 17.5 ONU remote alarm information

All onu alarm used this template configuration,

### 17.5.1 Showonu alarm information

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter the pon interface configuration mode. |
| **Step 3** | **show onu** <*onuid*> **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}** | Show ONU alarm status. |
| **Step 4** | **show onu** <*onuid*> **ctc alarm_thr onu {battery_volt_low\|onu_temp_high_alarm\|** | Show ONU alarm threshold. |

| | | |
|---|---|---|
| | **onu_temp_low_alarm}** | |

### 17.5.2 Show onu pon alarm information

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter the pon interface configuration mode. |
| **Step 3** | **showonu**<*onuid*>**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}** | Show pon optical power, temperature, voltage, current alarm status and threshold<br>alarm_cfg:onu alarm status<br>alarm_thr:onu alarm threshold |
| **Step 4** | **show onu** <*onuid*> **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\|** | Show the pon port statistical alarm status and threshold<br>alarm_cfg:onu alarm status<br>alarm_thr:onu alarm threshold |

| | |
|---|---|
| **downstream_jabbers_warning\|upstream_jabbers_warning\|downstream_discards_warning\|upstream_discards_warning\|downstream_errors_warning\|upstream_errors_warning}** | |

### 17.5.3 Show onu port alarm information

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter the pon interface configuration mode. |
| **Step 3** | **show onu** <*onuid*>**ctc alarm_cfg eth**<*1-255*>**{eth_port_auto_neg_failure\| eth_port_los\|eth_port_failure\|eth_port_loopback\|eth_port_congestion}** | Query port alarm status<br>alarm_cfg:onu alarm status |
| **Step 4** | **show onu**<*onuid*>**ctc{alarm_cfg\|alarm_thr}eth** <*1-255*>**{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\|** | Show the LAN port statistical alarm status and threshold<br><br>alarm_cfg:onu alarm status<br>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}** | |

### 17.5.4 Show onupots alarm information

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

### 17.5.5 Showonu E1 alarm information

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

## 17.6 ONU remote private oam configuration

### 17.6.1 Show ONU version of software|hardware

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configurationmode. |
| **Step 2** | **interface epon** *slot/port* | Enter the pon interface configuration mode. |
| **Step 3** | **show onu** *<onuid>***pri onu_ver** | Show ONUversion of software\|hardware |

### 17.6.2 Show ONU light and port status

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configurationmode. |
| **Step 2** | **interface epon** *slot/port* | Enter the pon interface configuration mode. |
| **Step 3** | **show onu** <*onuid*>**pri onu_status** | Show onu light and port status |

### 17.6.3 Configure MAC address aging time

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

### 17.6.4 Port maxMAC addresses

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

### 17.6.5 Show port MAC address table

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter the pon interface configuration mode. |
| **Step 3** | **show onu**<*onuid*>**pri** | Show port MAC address table |

| | | |
|---|---|---|
| | **eth**<*1-255*>**port_mac** | |

### 17.6.6 Port isolate enable|disable

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

### 17.6.7 Configure port negotiation mode

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

### 17.6.8 Show the port actually negotiation mode

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

### 17.6.9 Show port statistics

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter the pon interface |

| | | |
|---|---|---|
| | | configuration mode. |
| **Step 3** | **show onu** *<onuid>***pri eth** *<1-255>***ethernet_stat** | Show the port statistics of data packet |

### 17.6.10Configure port storm-control

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

### 17.6.11WiFi configuration

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

### 17.6.12SSID basic configuration

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter the pon interface configuration mode. |
| **Step 3a** | **onu** *<onuid>* **pri {wifi_ssid0\|wifi_ssid1\|wifi_ssid2\|wifi_ssid3** | Enable / disableSSID |

| | | |
|---|---|---|
| | **} {enable\|disable}** | |
| **Step 3b** | **onu** *<onuid>* **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}** | Name string: ssid string<br>hide [enable\|disable],enable:hide,disable: Don't hide<br>auth_mode:WLAN authentication mode<br>encrypt_type:WLAN encryption type |
| **Step 3c** | **onu** *<onuid>* **pri {wifi_ssid0\|wifi_ssid1\|wifi_ssid2\|wifi_ssid3}wpa shared_key** *<string>***rekey_interval** *<0-4194303>* | Shared_key: WPA Shared key, when authentication mode for WPAPSK or WPA2PSK, this configuration is effective.<br>Rekey_interval: WPA key update interval |
| **Step 3d** | **onu** *<onuid>* **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>* | Type: Type of the RADIUS server IP address<br>Len: the RADIUS server IP address length, authentication for WPA, connected, WPA/connected effectively<br>Ip: the RADIUS server Ip address, authentication for WPA, connected, WPA/connected effectively<br>Prefixlen: the RADIUS server address prefix length<br>Port: the RADIUS server Port<br>Key: the RADIUS server password |
| **Step 3e** | **onu** *<onuid>* **pri {wifi_ssid0\|wifi_ssid1\|wifi_ssid2\|wifi_ssid3}wep encryptionlevel {40\|104} keyindex** *<1-4>* **key1** *<string>***key2***<string>* **key3** *<string>* **key4** *<string>* | Encryptionlevel: WEP key length<br>Keyindex: key index, when encryption mode to WEP, this field is valid. key1-4:WEP keys 1-4 |
| **Step 3f** | **onu** *<onuid>* **pri {wifi_ssid0\|wifi_ssid1\|wifi_ssid2\|wifi_ssid3} wapi type{ipv4\|ipv6}serverip** *<ipstring>* **port** *<1-65535>* | Type:Type of wapi<br>Serverip:wapi ip address<br>Port:wapi port |
| **Step 3g** | **onu** *<onuid>* **pri {wifi_ssid0\|wifi_ssid1\|wifi_ssid2\|wifi_ssid3} commit** | Submit all configuration |

| | | |
|---|---|---|
| **Step 4** | **show onu** *<onuid>* **pri {wifi_ssid0\|wifi_ssid1\|wifi_ssid2\|wifi_ssid3 }** | show ssid configuration |

### 17.6.13Configure WAN connection

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

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

### 17.6.14Configure IGMP enable|disable

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter the pon interface configuration mode. |
| **Step 3** | **onu**<*onuid*>**pri igmp_admin***[enable\|disable]* | Configure IGMPenable\|disable |
| **Step 4** | **show onu** <*onuid*>**pri igmp_admin** | Show IGMP status |

### 17.6.15Configure CATV management

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

### 17.6.16Configure CTC OAM ignore

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

### 17.6.17Configure reset to default

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter the pon interface configuration mode. |
| **Step 3** | **onu**<*onuid*>**pri factory_reset** | Reset to default |

### 17.6.18Configure clean the MAC table

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter the pon interface configuration mode. |
| **Step 3** | **onu**<*onuid*>**pri mac_clean** | Configure clean the MAC table |

### 17.6.19Save the ONU configuration

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter the pon interface configuration mode. |
| **Step 3** | **onu**<*onuid*>**pri save_config** | Save the ONU configuration |

## 17.7 Show/Remove onu configuration

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter the pon interface configuration mode. |
| **Step 3** | **show onu running-config** | 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3a** | **no onu** <*onuid*>**{upstream\|downstream}** | Remove ONU upstream or downstream bandwidth configuration. |
| **Step 3b** | **no onu** <*onuid*> **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}** | Remove ONU global configurations. |
| **Step 3c** | **no onu** <*onuid*> **ctc eth** {<*1-255*>\|**all}{flow_control\|policy\|rate_limit\|loopdetect\|disableloop\|monitor_status\| monitor_current\|vlan\|class\|mc_vlan\|mc_tagstrip\|mc_maxgrp\|phy_ctrl\|autoneg\|pvid }** | Remove ONU LAN configuration. |
| **Step 3d** | **no onu** <*onuid*> **ctc pots** {<*1-255*>\|**all}{h248_user_tid\|sip_user_config\|port_manage}** | Remove ONU POTS configurations. |
| **Step 3e** | **noonu**<*onuid*>**pri {age_time\|wifi_switch\|wifi_ssid0\|wifi_ssid1\|wifi_ssid2\|wifi_ssid3\|wan_conn}** | Remove ONU private OAM configured parameters. |
| **Step 3f** | **no onu** <*onuid*> **pri eth** <*1-255*>**{pkg_suppress\|mac_limit}** | Remove ONU private OAM configured LAN parameters. |

## 17.8 ONU template management

### 17.8.1 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

### 17.8.2 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **profile dbaadd** *{<1-32767>}*1* | Create a DBA template |
| **Step 3** | **profile dbaid**<*1-32767*> | Enter the DBA template node |
| **Step 4** | **modify fir**<*0-950000*>**cir**<*1-950000*>**pir**<*512-1000000*>**weight**<*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** | **commit** | Commit the template configuration |
| **Step 6** | **exit** | Exit template node |
| **Step 7** | **interface epon** *slot/port* | Enter the pon interface configuration mode. |
| **Step 8** | **onu**<*onuid*>**profile dba id**<*1-32767*> | Binding the dba template to set corresponding onu |
| **Step 9** | **show onu**<*onuid*>**profile_id** | Query the onu binding template accordingly |
| **Step 10** | **exit** | Exit the pon interface node |
| **Step 11** | **show profile dba id**<*0-32767*> | Show template configuration |
| **Step 12** | **show profile dba id**<*0-32767*>**bind** | Show onu bindings in the template |
| **Step 13** | **no profile dba id**<*1-32767*> | Delete the dba template |

### 17.8.3 Services(SRV) template configuration

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

The SRV template has the following configuration:

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

modify [lan_count] <0-255>

**2.Multicastfast leave**

modifyctc fast_leave [enable|disable]

**3.FEC**

modifyctc fec_mode [enable|disable]

**4.Multicast mode**

modifyctc [mc_switch] [snooping|control]

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

modifyctc [multi_llid] <0-8>

**6.Pon number(s)**

modifyctc [active_pon] <0-8>

**7.Optical link protectio**

modifyctc [holdover] <0-65535>

**8.Onu management IP address**

modifyctc [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_bandwith <0-1024> guaranteed-bandwidth <1-1024> best_effort_bandwith <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]
modifypri [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> [tranlation] [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|tranlation|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] broddcast <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** | **configure terminal** | Enter global configuration mode.. |
| **Step 2** | **profile voip add** *{<1-32767>}*1* | Create the VoIP template |
| **Step 3** | **profile voip id**<*1-32767*> | Enter the VoIP template node |
| **Step 4** | **modify pots_count**<*0-255*> | Configure lan port quantity of template |
| **Step 5** | **commit** | Commit the template configuration |
| **Step 6** | **exit** | Exit template node |

| | | |
|---|---|---|
| **Step 7** | **interface epon** *slot/port* | Enter the pon interface configuration mode. |
| **Step 8** | **onu**<*onuid*>**profile voip id**<*1-32767*> | Binding the VoIP template to set correspondin |
| **Step 9** | **show onu**<*onuid*>**profile_id** | Query the onu binding template accordingly |
| **Step 10** | **exit** | Exit the pon interface node |
| **Step 11** | **show profile voip id**<*0-32767*> | Show template configuration |
| **Step 12** | **show profile voip id**<*0-32767*>**bind** | Show onu bindings in the template |
| **Step 13** | **no profile voip id**<*1-32767*> | 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|unalign] 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 ctc [fax_modem_config] voice_t38 [enable|disable] control [negotiation|auto_vbd]

7.OnuSIP digitmap

modify ctc [sip_digit_map] num <0-255><0-255><mapstr>

8.OnuPOTS port userTID information

modify ctc pots <1-255> [h248_user_tid] <name>

9.OnuPOTS port user account information

modify ctc pots <1-255> [sip_user_config] account <account> name <name> pwd <password>

10.Remove configuration instructions

no ctc [voip_global_param|h248_param_config|h248_rtp_tid|sip_param_config|fax_modem_config|sip_digit_map]

no ctc pots <1-255> [h248_user_tid|sip_user_config]

### 17.8.4Alarm threshold template configuration

Alarm thresholdonly can be configured by template. Begin at privileged configuration mode, configure alarm threshold template as the following table shows.

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

Alarm template has the following configuration:

1.Disable onu alarm

modifyctc [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.Enabld 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& Clear onu temperature alarm

modify ctc [onu] [onu_temp_high_alarm|onu_temp_low_alarm] [enable] <alarm><clear>

4.Enable onu voltage alarm

modify ctc [onu] [battery_volt_low] [enable] <0-65535><0-65535>

5.Disable 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.Enabld 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 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 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.Enablepon 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_los|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/Disablepots alarm**

modifyctc [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_los] [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_hig

h_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_u
ndersize_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_ev
ents_warning|downstream_crcerror_frames_warning|downstream_undersize_frames_w
arning|upstream_undersize_frames_warning|
downstream_oversize_frames_warning|upstream_oversize_frames_warning|downstrea
m_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_los|eth_port_failure|eth_port_loopback|eth_port_c
ongestion]
no ctc [eth] <1-255> [downstream_drop_events_alarm|upstream_drop_events_alarm|
downstream_crcerror_frames_alarm|downstream_undersize_frames_alarm|upstream_u
ndersize_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|upstrea
m_undersize_frames_warning|downstream_oversize_frames_warning|upstream_oversiz
e_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_los]

### 17.8.4 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** | **configure terminal** | Enter global configuration mode.. |
| **Step 2** | **interface epon** *slot/port* | Enter the pon interface |

| | | |
|---|---|---|
| | | configuration mode. |
| | **Onu**<auto-bind>**profile** [dba\|srv\|voip\|alarm] **id** <0-32767> | Config thetemplate auto bind to set corresponding. |
| **Step 3a** | **show** <onu><*auto-bind*>**profile_id** | Show auto bind template. |

### 17.8.5 Show/RemoveONU template configuration

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode.. |
| **Step 2** | **no profile {dba\|srv\|voip\|alarm}id** *<1-32767>* | Delete the template |
| **Step 3a** | **show profile{dba\|srv\|voip\|alarm} all\|id** *<0-65535>***}** | Show template configuration. |
| **Step 3b** | **show profile {dba\|srv\|voip\|alarm} id** *<0-65535>***bind** | Show the template id binding onu |

# 18.System Management

## 18.1 Configuration file management

### 18.1.1 Save configurations

After modified the configurations, you should same them so that these configurations can take effect next time it restarts. Use the following commands to save configurations.

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **write** | Save configurations. |

### 18.1.2 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **erase startup-config** | Erase all configurations. |

### 18.1.3 Show startup configurations

Use the following command to display the configurations you have saved.

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **show startup-config** | 显示已保存的配置 |

### 18.1.4 Show running configurations

Use the following commands to display running configurations. These running configurations may not be saved in flash.

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **show running-config** | Show running configurations. |

### 18.1.5 Upload/download configuration file

Use the following commands to upload configuration file to PC and download configuration file to device.

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **debug mode** | Enter debug node |
| **Step 3a** | **upload tftp configuration**<*filename*><*A.B.C.D*> | filename is Upgrade file A.B.C.D is TFTP server IP |
| **Step 3b** | **download tftp configuration**<*filename*><*A.B.C.D*> | filename is Upgrade file A.B.C.D is TFTP server IP |

## 18.2 Check the system information

### 18.2.1 Check system running information

Use the following commands to view system information.

| Command | Function |
|---|---|
| **show sys arp** | Show ARP table |
| **show sys cpu** | Show CPU information |
| **show sys cpu-usage** | Show CPU usage rate |
| **show sys mem** | Show system memory |
| **show sys ps** | Show system process |
| **show top** | Show CPU utilization |
| **show task** | Showthread name |

### 18.2.2 Check version information

Use the following commands to check version information which includes hardware version, software version, software created time and so on.

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **show version** | Show version information. |

### 18.2.3 Check system running time

Use the following command to show system running time after turned power on.

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **show sys running-time** | Show system running time. |

## 18.3 System basic configurations

### 18.3.1 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **hostname**<*name*> | Configure system name. It must start with alphabet. |
| **Step 3** | **hostname default** | 恢复默认系统名 |

### 18.3.2 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 attribure as the followingtable shows.

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **terminal length** *value* | Configure display line number. Value range is 0-512. |

### 18.3.3 Configure terminal time-out value

Use the following commands to configure terminal time-out value. Default value is 10 minutes.

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **line vty** | Enter line node |
| **Step 3a** | **exec-timeout** <*min*> *[*<*second*>*]* | Set the command-line timeout |
| **Step 3b** | **no exec-timeout** | Set the command-line timeout to default |
| **Step 4** | **show exec-timeout** | Show the command-line timeout |

## 18.4 System basic operations

### 18.4.1 Upgrade system

Use the following command to upgrade the equipment.

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2b** | **download tftp image**<*filename*><*A.B.C.D*> | Update firmware with header. |

### 18.4.2 Network connectivity test

Use **ping** command to check network connectivity.

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **ping** [**-s**<*packetsize*>]<*A.B.C.D*> | *Packetsize* is test packet length, unit is byte. |

### 18.4.3 Reboot system

Use the following command to reboot system.

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **reboot** | Reboot system. |

### 18.4.4 Telnet

You can telent to system via outband or inband management IP. The default outband management IP is 192.168.8.100.

| Command | Function |
|---|---|
| **telnet 192.168.100** | Telnet to application layer of system. Login name and passwork both are **admin**. |
| **telnet 192.168.100 2223** | Telnet to kernel of system. Login name is **default**. |
| epon-olt(config)#**switch** | Telnet to kernel of system. Login name is **default**. |

### 18.4.5 Configure RTC system time

Use the following command to configure RTC system time.

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |

| | | |
|---|---|---|
| **Step 2** | **time set year** *<2000-2099>* **month***<1-12>* **day***<1-31>* **hour***<0-23>* **minute** *<0-59>* **second** *<0-59>* | Configure the RTC clock |
| **Step 3** | **show time** | Show the system time |

### 18.4.6 Fan control

Use the following command to control fan running attribute.

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **fan temperature** *<20-80>* | Configure Temperature of the fan |
| **Step 3** | **fan mode [open\|close\|auto]** | Configure the fan open mode |
| **Step 4** | **show fan** | Show the fan configuration and current equipment temperature |

## 18.5 OAM debug information

### 18.5.1 Enable/disable OAM debug information

Use the following commands to enable or disable OAM debug information.

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **debug mode** | Enter debug node |
| **Step 3** | **config level view {recv_pkt\|recv_from_onu_pkt\|recv_from_cs8022_pkt\|send_pkt\|send_to_onu_pkt\|send_to_cs8022_pkt\|oam_pkt\|oam_time}{on\|off}** | 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 |

### 18.5.2 Enable/disable CPU debug information

Use the following commands to enable or disable CPU debug information.

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **debug mode** | Enter debug node. |
| **Step 3** | **system debug {rx\|tx}{on\|off}** | On\|off : enable or disable CPU debug.<br>Rx: CPU receives packets.<br>Tx: CPU transmits packets. |

### 18.5.3 Enable/disable each function module debug information

Use the following commands to enable or disable function module debug information.

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **debug mode** | Enter debug node. |
| **Step 3** | **system debug {acl\|timer\|port\|mac\|vlan\|vt\|igmp\|cfp\|qos}{ on\|off}** | On\|off : enable or disable function module debug information. |

# 19 User Management

## 19.1 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.

## 19.2 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.

## 19.3 Add user account

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **user add** *user-name* **login-password** *login-password* | Add new user account. |
| **Step 3** | **user role** *user-name*{**admin** \|**normal** **enable-password***enable-password*} | Specify user role. New user is a normal privilege user. |

## 19.4 Show user account list

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **user list** | Show user account list. |

## 19.5 Delete user account

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |

| | | |
|---|---|---|
| **Step 2** | **user delete** *username* | Delete user account. |

## 19.6 Modify password

Every user can modify its own password while administrator user can modify other users' password. Modify password as the following table shows.

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **user login-password** *user-name*<CR><br>Input new login password for user abc please.<br>New Password:<br>Confirm Password: | Configure user's login password. |
| **Step 3** | **user enable-password** *user-name*<CR><br>Input new enable password for user abc please.<br>New Password:<br>Confirm Password: | Configure user's configuration mode password. |

# 20 SNMP Configuration

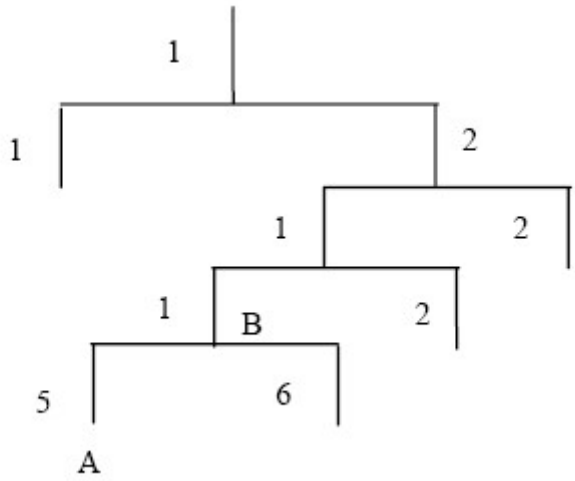
## 20.1 SNMP introduction

SNMP (Simple NetworkManagement 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 resports. 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.

## 20.2 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.

GEPON 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 | |

## 20.3 Configure SNMP

### 20.3.1 Configure community

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

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **config terminal** | Enter global configuration mode. |
| **Step 2** | **snmp-server community** <*word*> **[ro\| rw]** | Configure SNMP community strings; |
| **Step 3** | **show snmp-server community** | Show the SNMP community configuration |
| **Step 4** | **exit** | From the global configuration mode to return to the privileged user configuration mode |
| **Step 5** | **write** | Save the configuration |

### 20.3.2 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 addressas the following table shows.

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **config terminal** | Enter global configuration mode. |
| **Step 2a** | **snmp-server host <***A.B.C.D***>{udp-port** <*1-65535*>**}*1 {version [1\|2c]}*1 {**community** <*WORD*>**}***1 | Configure the Trap the target host address.<br>Configure the community string value |
| **Step 2b** | **no snmp-server host** < *A.B.C.D* > **version 1\|2c\|3***community* | Delete trap target host address. |

| | | |
|---|---|---|
| **Step 3a** | **snmp-server enable traps snmp** | Enable SNMP traps function |
| **Step 3b** | **no snmp-server enable traps snmp** | Delete SNMP traps function |
| **Step 4** | **show snmp-server targetaddress** | Check the SNMP trap configuration |
| **Step 5** | **write** | Save the configuration |

### 20.3.3 ConfigureAdministrator ID and contact method

Begin at privileged configuration mode, Configure administrator ID and contact mwthodas the following table shows.

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **config terminal** | Enter global configuration mode. |
| **Step 2** | **snmp-server contact**<*line*> | Configure contact string value |
| **Step 3** | **show snmp-server contact** | Check the SNMP contact configuration. |
| **Step 4** | **write** | Save the configuration. |

### 20.3.4 Configure Ethernet switch location information

Begin at privileged configuration mode, Configure Ethernet switch location information as the following table shows.

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **config terminal** | Enter global configuration mode |
| **Step 2** | **snmp-server location**<*line*> | Configure location string value |
| **Step 3** | **show snmp-server location** | Check the SNMP location configuration. |
| **Step 4** | **write** | Save the configuration. |

# 21 Alarm and Event Management

## 21.1 Alarm and event introduction

If you enable alarm report, it will trigger alarm events when system occured 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 secury 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.

## 21.2 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 conflication, ONU LOID conflication, 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.

### 21.2.1 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2a** | **alarm {temp-high\|temp-low\|cpu-usage-high\|mem-usage-high} disable** | Disable system alarm report. |
| **Step 2b** | **alarm {temp-high\|temp-low\|cpu-usage-high\|mem-usage-high} enable** *<alarm-value><clear-value>* | Enable system alarm report and configure system alarm threshold.<br>alarm-value: alarm threshold.<br>clear-value: clear threshold. |
| **Step 2c** | **alarm {fan\|port-updown\|port-loopback\|register-failed\|deregister}{enable\|disable}** | Enable or disable system alarm report. |
| **Step 3** | **show alarm configuration** | Show system alarm configurations. |

### 21.2.2 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2a** | **alarm {pon-register-failed\|pon-deregister}{enable\|disable}** | Enable or disable PON alarm report. |
| **Step 2a** | **alarm {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}** | Enable or disable PON port alarm report. |
| **Step 3** | **show alarm configuration** | 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface epon** *slot/port* | Enter PON interface configuration mode. |
| **Step 3a** | **alarmpon optical{tx_power_high\|tx_power_low\|tx_bias_high\|tx_bias_low\|vcc_high\|vcc_low\|temp_high\|temp_low} disable** | Disable PON port alarm report. |
| **Step 3b** | **alarm pon optica {tx_power_high\|tx_power_low \|tx_bias_high \|tx_bias_low\|vcc_high** | Enable PON port alarm report and configure alarm parameters. |

| | | |
|---|---|---|
| | **\|vcc_low \| temp_high\|temp_low}enable** *<alarm-value><clear-value>* | alarm-value: alarm threshold. clear-value: clear threshold. |
| **Step 4** | **show alarm pon optical configuration** | 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** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **alarm {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}** | Enable or disable ONU alarm report. |
| **Step 3** | **show alarm configuration** | Show system alarm configurations. |

## 21.3 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 diposing 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, ungrade successful and so on.

### 21.3.1 System events

System events are mainly used to monitor performation 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** | **configure terminal** | Enter global configuration mode. |
| **Step 2a** | **event reset {enable\|disable}** | Enable or disable system event report. |
| **Step 3** | **show event configuration** | Show system event configurations. |

### 21.3.2 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 |

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **event {pon-register\|pon-los-recovery}{enable\|disable}** | Enble or disable PON event report. |
| **Step 3** | **show event configuration** | Show system event configurations. |

### 21.3.3 ONU events

ONU events also can help administrator to get rid of some ONU fault. The following table shows ONU event list.

| ONU event | Reason | Default |
|---|---|---|
| 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 |

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2b** | **event {onu-register\|onu-link-discover\| onu-auth-success\|onu-deauth-success}{enable\|disable}** | Enable or disable ONU event report. |
| **Step 3** | **show event configuration** | Show system event configuration. |

# 22 OAM Interactive Information Manangement

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.

## 22.1 Configurelog output level of modules

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **debug mode** | Enter debug node |
| **Step 3** | **config level print {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** | **display level print {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 |

## 22.2 Configure log store level of modules

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **debug mode** | Enter debug node |
| **Step 3** | **config level 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\|ess_vlan}**<*0-7*> | Configure modules log memory store level |
| **Step 4** | **display level log** | Show modules log memory |

| | | |
|---|---|---|
| | **{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}** | store level |
| **Step 5a** | **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\|ess_vlan}** | Display module stored in the memory of the log information |
| **Step 5b** | **display log level**<*0-7*> | Display log information stored in the memory module at all levels |
| **Step 5c** | **display log{latest\|oldest}**<*1-1024*> | Display log information |
| **Step 6a** | **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\|ess_vlan}** | Delete all modules are stored in the memory of the log information |
| **Step 6b** | **delete log level** <*0-7*> | Delete all the log information stored in the memory module at all levels |

# 23 System Log

## 23.1 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 deivce 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.

### 23.1.1 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.

### 23.1.2 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 |

## 23.2 Configure system log

### 23.2.1 Show system log

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **Show syslog[level {debug\|info\|notice\|warning\|major\|critical\|alert\|emerg}]** | Show all system log or log of specific level. |

### 23.2.2 Clear system log

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **Clear syslog[level {debug\|info\|notice\|warning\|major\|critical\|alert\|emerg}]** | Clear all system log or log of specific level. |

### 23.2.3 Configure system log server

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2a** | **syslog server ip** *<A.B.C.D>* **port** *<1-65535>* | Configure system log server IP and port. |
| **Step 2b** | **no syslog server** | Delete system log server configuration. |
| **Step 3** | **show syslog server** | Show system log server configuration. |

### 23.2.4 Configure save level of system log

| | Command | Function |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |

| | | |
|---|---|---|
| **Step 2** | **syslog flash level {debug\|info\|notice\|warning\|major\|critical\|alert\|emerg}** | System log will be saved to flash if it is higher than you set. |
| **Step 3** | **show syslog flash level** | Show system log level in flash. |

### 23.2.5 Save system log to flash

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **save syslog flash** | Save system log to flash. |

### 23.2.6 Clear system log in flash

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **clear syslog flash** | Clear system log in flash. |

### 23.2.7 Upload system log

| | **Command** | **Function** |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **upload tftp syslog** *<filename><A.B.C.D>* | Upload system log to local host byTFTP. |