



AX3500 XGSPON OLT CLI Operation

QRG

Revision B

ACT AX3500 XGSPON OLT CLI Operation QRG

ACT Document Number: ACT AX3500 XGSPON OLT CLI Operation QRG

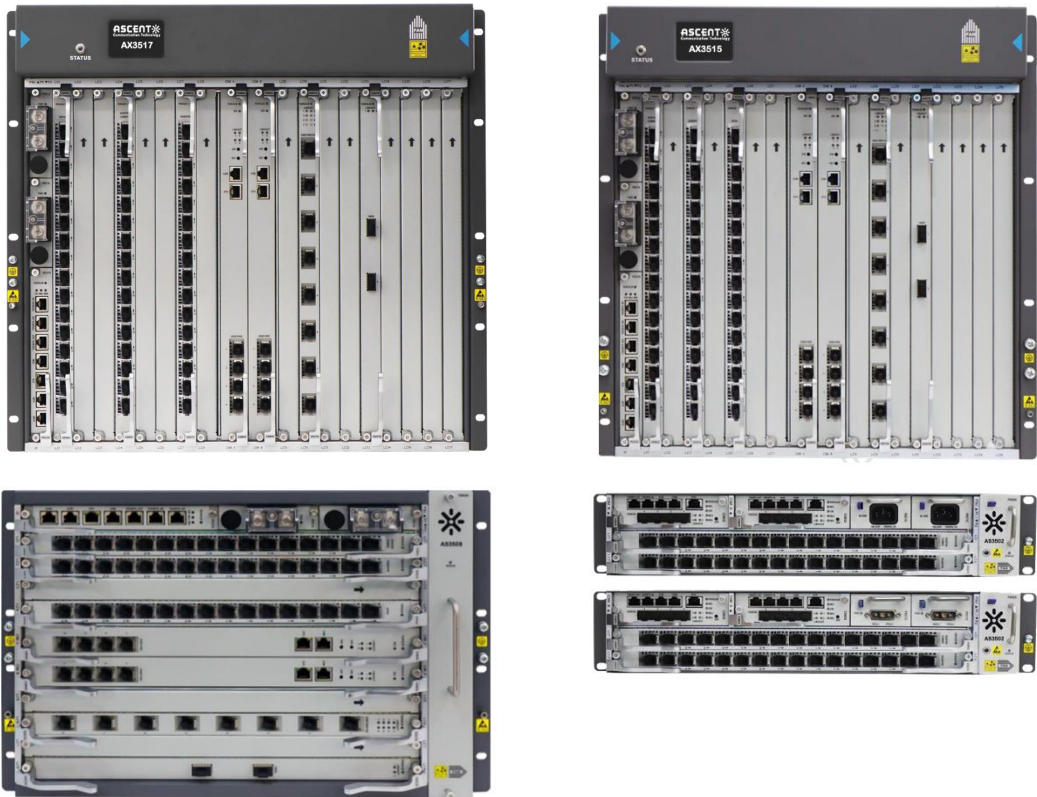
Quick Reference Guide Revision B

Copyright © 2025 Ascent Communication Technology Limited.

All rights reserved. Reproduction in any manner whatsoever without the express written permission of Ascent Communication Technology is strictly forbidden.

This document is produced to assist professional and properly trained personnel with installation and maintenance issues for the product. The capabilities, system requirements and/or compatibility with third-party products described herein are subject to change without notice.

For more information, contact ACT: support@ascentcomtec.com



Revision History

Revision	Date	Reason for Change
A	02/24/2023	Initial release
B	06/28/2025	Update format

Table of Contents

1 Command Line Interface	8
1.1 Terminal Emulation Login	8
1.2 Telnet Login	9
1.3 SSH2 Login	10
1.4 Session Login	10
1.5 Log Off	10
1.6 CLI Command Mode	11
1.7 CLI Grammar Specification	12
1.8 CLI Command Help	13
1.9 Keyboard Shortcut	14
2 Startup OLT Product	14
2.1 AX3500 Series Product Introduction to System Interface	15
2.2 Configure Basic Data Service Concept	15
2.3 Configure Basic Data Service Instance	16
3 System Configuration	20
3.1 In-Band and Out-of-Band Introduction	20
3.2 Configure Basic System Information	22
3.3 SNMP Initialization Configuration	23
3.4 Configure SNTP	25
3.5 Alarm	26
3.6 Node Access Control	33
3.7 LLDP	34
3.8 AAA Authentication	36
3.9 802.1x	38
4 L2 Configuration	42

4.1 SVI Concept	42
4.2 Mac Address Table	44
4.3 Link Aggregation	44
4.4 Link Aggregation	45
4.5 Port Mirror	48
4.6 RSTP.....	49
4.7 MSTP	50
4.8 Relay Options	51
4.9 Loop Detection.....	51
5 L3 Configuration.....	52
5.1 SVI Concept	52
5.2 Create SVI.....	53
5.3 Configure ARP	53
5.4 Configure IP Route	54
6 GPON Configuration.....	54
6.1 Configure ONU Authentication.....	54
6.2 Configure ONU Registration	55
6.3 Configure ONU Service	57
6.4 OLT Management.....	66
6.5 ONU Management.....	67
6.6 FEC.....	75
6.7 Encryption	76
6.8 PON Protection	77
6.9 PON Optical Power Monitor	80
6.10 Rogue ONU Detection.....	82
6.11 EasyPON	83
6.12 PON Energy Saving.....	84
6.13 ONU Automatic Registration	84
6.14 Automatically Register and Apply Templates	85
6.15 ONU WAN port configuration or Wi-Fi configuration	86

6.16 ONU SNTP	86
7 Multicast Configuration	87
7.1 IP Multicast Introduction	87
7.2 IGMP Snooping Introduction	87
7.3 IGMP Configuration Instance	87
7.4 Enable MLDv2 Proxy	92
7.5 Check MLD Proxy	95
8 ACL	95
8.1 Application Description	95
8.2 Operating Steps	95
9 QoS	96
9.1 Introduction	96
9.2 Rate Limit	97
9.3 Queue Mapping	97
9.4 DSCP Mapping	97
9.5 Scheduling Mode	97
9.6 Weight Configuration	97
9.7 Egress Queue Metering	98
9.8 Drop Priority Map	98
9.9 Flow-Based QoS	98
10 SyncE	99
10.1 Introduction	99
10.2 SyncE Configuration Instance	99
11 PTP	101
11.1 Introduction	101
11.2 Principles of GPON Transmission Time	105
11.3 PTP Configuration Instance	107
12 External Alarm Input/Output	116

12.1 Introduction	116
12.2 Product Specifications	116
12.3 Operating Steps	116
13 Security	119
13.1 DHCP Snooping	119
13.2 PPPOE Snooping.....	120
13.3 Anti-MAC-Spoofing	120
13.4 ARP Snooping	120
13.5 IP-MAC-Bind	120
13.6 MAC Force Forwarding	121
14 Performance Statistics	121
14.1 View Performance Statistics	121
14.2 Clear Performance Statistics	122
15 System Administration	122
15.1 Equipment Document Management	122
15.2 Save Configuration	123
15.3 Reboot System	123
15.4 Active-Standby Switchover	123
15.5 System Upgrade	123

About This Guide

Introduction

This document describes the configuration procedures of AX3500 XGSPON series OLTs through Command Line Interface (CLI).

Audience





- System administrators
- Installation engineers
- Operation engineers
- Maintenance engineers
- Troubleshooting and repair engineers
- Service engineers

Conventions

This guide may contain notice icons, figures, screen captures, and certain typographical conventions. These conventions are described below.

Notice Icons

The following table lists notice icons used in this guide.

Icon	Notice Type	Description
	Note	A note providing important information or instructions but is not hazard-related.
	Caution	Information to alert of potential damage to a program, data, system, or device. If not avoided, may result in minor or moderate damage. It may also alert against unsafe practices and potential program, data, system, or device damage.
	Warning	Information to alert of operations that may cause an accident, personal injury, fatality or potential electrical hazard. If not avoided, could result in serious injury or even death.
	ESD	Special handling instructions for components sensitive to electrostatic discharge damage.

Typographical Conventions

The following table lists typographical conventions used in this guide.

Convention	Description
Text displayed in the Courier New Font	This typeface represents text that appears on a terminal screen, including, system information output, command prompts, and user typed commands. Commands typed by users are in bold. Example: telnet@hostname>enable.
Text in bold	Bold text represents window names, user interface control names, function names, user typed commands, and directory and file names. Example: Set the Time field.
Text enclosed in [square brackets]	Text enclosed in square brackets represents menu items such as [File] and [File > New].
Text enclosed in <angle brackets>	Text enclosed in angle brackets represents user interface buttons and keyboard function keys. Example: Click <OK>.
Text in <i>italics</i>	Text in italics represents the names of reference documents. Example: Refer to the <i>Rack Installation Guide</i> .

Figures and Screen Captures

This guide provides figures and screen captures as examples. These examples contain sample data which may differ from the actual data on an installed system.

How to Comment on This Guide

To provide comments on this documentation, send an e-mail to: sales@ascentcomtec.com. Please include the name of the guide being referenced. If applicable, provide the chapter and page number.

1 Command Line Interface

Users can use the following different management interfaces for network management:

- SNMP management
- CLI based management

This manual introduces the CLI configuration function of AX3517/AX3515/AX3508/AX3502 system. In the initial setup phase of AX3517/AX3515/AX3508/AX3502, the following two methods based on cli management can be used to log in to the system:

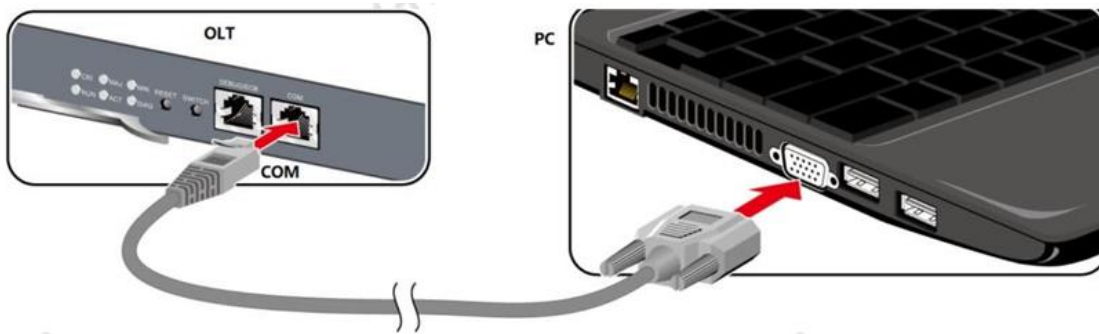
- Terminal simulation using debug port (RJ-45 connector)
- Telnet using management port (RJ-45 connector)

1.1 Terminal Emulation Login

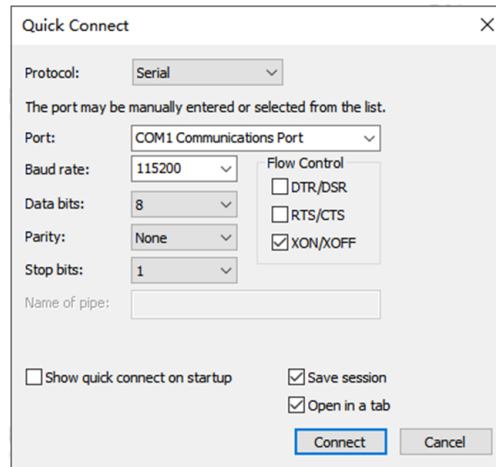
When using terminal emulation to access the AX3517/AX3515/AX3508/AX3502 system, the PC's serial RS-232 COM port is connected to the /AX3515/AX3508/AX3502 DEBUG port. Follow the steps below to connect a PC to the AX3517/AX3515/AX3508/AX3502 system.

1. Use a RJ-45/DB9 RS-232 serial cable. Connect the DB-9 connector to a vacant serial RS-232 COM port on the PC, and the RJ-45 connector to the AX3517/AX3515/AX3508/AX3502's DEBUG port, as shown in below figure.

Connection of RJ-45 / DB9 RS-232 serial port cable figure



2. Start a terminal emulation program, in this example, SecureCRT is used.
3. Select [File/Quick Connect] from the secureCRT main menu. The Quick Connect dialog box pops up.




4. Set the communication parameters to the following values:

- BitsperSecond:115200
- Data Bits: 8.
- Parity: None
- Stop Bits: 1
- Flow Control: None

5. Click <Connect> to complete the setup.

If the cable and terminal communication parameters are setup correctly, the system will prompt you for the Username and Password.

10.20.30.1 login:

 **Note:** The default system administrator username and password are: **admin** and **admin**.

6. Type the user name and password.


After logging on to AX3517/AX3515/AX3508/AX3502 successfully, the following command prompt appears.

AX3517#

1.2 Telnet Login

When using Telnet to access the AX3517/AX3515/AX3508/AX3502 system, the PC network card's (RJ-45) connector is connected to the AX3517/AX3515/AX3508/AX3502's Management port (RJ-45). Follow the steps below to connect a PC to the AX3517/AX3515/AX3508/AX3502 system:

Use an Ethernet cable with RJ-45 connectors on both ends to connect the AX3517/AX3515/AX3508/AX3502 Management port (ETH) with the PC's network card.

 **Note:** The AX3517/AX3515/AX3508/AX3502 management port supports Auto-MDIX, so either a straight-through or crossover cable can be used.

- Configure the PC's static IP address to be in the same subnet as the default AX3517/AX3515/AX3508/AX3502 Management port IP address (10.20.30.1). [Example:10.20.30.2]
- From the Windows Start menu, select [Start>Run]. Type the following command:

C:\ telnet 10.20.30.1



Note: For AX3517/AX3515/AX3508/AX3502, the default administrator username and password are both "**admin**".

- Type the Username and Password.

Upon successful log on, the following system prompt appears.

AX3517#

This prompt indicates that the user is connected at the first command mode interface; the EXEC level.

The EXEC level is the base command mode entered when first logging on to the AX3517/AX3515/AX3508/AX3502 system. From this command mode a user can view but not modify system properties. If the user's account privileges allow, the user can access one of the other command modes to perform system configuration functions.



Note: For more information on user account privilege, refer to Section CLI Command Mode.

1.3 SSH2 Login

AX3517/AX3515/AX3508/AX3502 system support to remote access Secure Shell (SSH) version 2, and not support SSH V1.

1.4 Session Login

The idle session timeout is set to 5 minutes by default. When a session has been idle for 5 minutes, the user will automatically be logged out.

To change the idle time-out duration, follow the steps below:

- Execute the following command to set the idle session timeout to one hour.

AX3517# access idle-timeout 3600



Note: The timeout range is 60 to 100000 seconds.

- Issue the command below to save the new configuration.

AX3517# save config

Are you sure you want to save the configuration ? (yes or no)

Enter "y" to confirm.

After issuing the save command, the configuration information is saved in the AX3517/AX3515/AX3508/AX3502's Flash memory. It normally takes several seconds before the configuration is saved. After the configuration is saved successfully, the following command prompt is displayed to indicate that the time-out configuration was successful.

AX3517#

1.5 Log Off

There are two different CLI log off types: Manual Log off and Time-out.

- **Manual Log off:** At any command mode, type the logout command to terminate the current CLI connection.
- **Time-out:** A time-out occurs when the user account has been idle for the configured Idle Timeout period.

1.6 CLI Command Mode

The AX3517/AX3515/AX3508/AX3502 CLI utilizes a layered command architecture referred to as command modes. Each of these command modes provides a subset of CLI commands. The CLI commands available depends on which command mode is currently active.

When the user logs in for the first time, it is in the basic configuration mode, and the command mode is as follows.

1.6.1 System Configuration

This command mode allows the user to change the basic configuration of the device. Including system parameter configuration.

1.6.2 Configuration Mode

This command mode allows the user to change the global configuration. The configure command mode at the root level, also known as the global configuration command mode, includes function profiles, L2, L3 and other configurations.

Access method: configure prompt in OLT

AX3517#Execute the config command after

Enter the corresponding function configuration mode according to different functions: example:

AX3517(CONFIG)#l2

AX3517(CONFIG/L2)#vlan AX3517(CONFIG/L2/VLAN)#

1.6.3 Master Based Global Configuration

AX3517/AX3515/AX3508/AX3502 directly configures the master card and line card based on the master card.

1.6.3.1 Line Card Configuration

Line card access method: configure prompt in OLT execute the **slot < slot ID >**

command after AX3517#.

Explain: AX3517# slot 3

The system prompt is AX3517(Slot-3)#

1.6.3.2 Line Card OLT Configuration

Access method of line card OLT: execute interface GPON OLT < module / port > command after

AX3517 (slot-3) # to enter this mode.

AX3517(Slot-3)#interface gpon-olt 1/2

AX3517(Slot-3/if-gpon-olt-1/2)#

Exit method: enter exit in the current command mode.



Explain: In the above command, "1" means the first level of the slot, "2" means the PON port number of the line card is 2. For AX3517/AX3515/AX3508/AX3502 devices, after entering the slot, the slot level is fixed to 1, and the PON port number is based on the actual port serial number.

1.6.3.3 Line Card ONU Configuration

ONU configuration mode is a sub mode of OLT configuration command mode, which is used to configure ONU parameters.

Access method: execute ont < ONU ID > command after OLT configuration prompt

AX3517 (slot-13 / if GPON OLT -- < module / port >) # to enter this mode. Example:

AX3517(Slot-3/if-gpon-olt-1/1)# onu 31

The system prompt is AX3517(Slot-3/if-gpon-olt-1/2/31)#

Exit method: enter **exit** in the current command mode.



Explain: In the above prompt, "1/2/31" indicates OLT 3 slot level 1, PON port number 2 and ONU ID number 31, respectively, and these numbers are based on the actual port and ONU ID.

1.7 CLI Grammar Specification

CLI commands include the command itself and required and / or optional keywords and parameters. To accurately represent the complete cli commands, use the following specifications.

- Example 1:

Grammar: **snmp-server community** <text-string> {ro|rw} enable|disable

- Example 2 :

Grammar: **static-mac-address** <MAC-addr> {vlan <VLAN-ID>} {port <port-num>} [cos <value>]

Explain

- Bold characters represent the command itself or command keywords
- The text in "< >" is a required parameter
- The text in '{}' is a required parameter with keywords
- The text in '[]' is an optional parameter
- Text other than "< >" or "[]" is the command keyword or the command itself

According to the specifications defined above, for the command status MAC address, < MAC addr > is a required parameter, {VLAN < VLAN ID >} is a required parameter with keywords, and [cos < value >] is an optional parameter (COS is a keyword). Enable|disable in the first command is a required parameter for multiple selections.

1.8 CLI Command Help

The AX3517/AX3515/AX3508/AX3502 CLI provides various help and shortcut keys. Below table lists the main shortcuts and methods for accessing help within the CLI.

Field	Description
Enter "?" at any cli command level	All available commands in the present command modes are displayed.
Enter some commands + "?"	All commands beginning with the text entered are displayed. (Do not enter a space before the question mark.)
Command + space + "?"	The complete syntax and brief description of the command appears.
Enter some commands + < tab >	The system automatically completes the command or keyword.
If the command and / or keyword entered is incomplete, but it is long enough for the system to recognize the command	Then the system will execute this partial command, which is the same as the complete command.
Enter "tree" at any cli command level	All available commands in the present command mode are displayed in a list.
"Ctrl-p" or up cursor key ↑	Invoke a previously issued command. The last 20 commands are available.
History	Open a list of the last 30 commands issued.

Example 1:

```
AX3517# ?
access          - Enter access configuration mode
alarm           - Enter Alarm configuration mode
auto-correction - Enable CLI auto correction mode
banner          - Configure login banner
```

Example 2:

```
AX3517(CONFIG)#sec?
Security
AX3517(CONFIG)#security
```

Example 3:

```
AX3517# conf + <Tab>
AX3517# configure
```

1.9 Keyboard Shortcut

Field	Description
Ctrl-Z	The command entered before pressing Ctrl-Z is issued and the command mode returns to the EXEC command mode. If a command is not entered, the command mode state returns to the EXEC command mode.
Ctrl-B, Left cursor key	Move the cursor left without deleting characters
Ctrl-F, Right cursor key	Move the cursor one character to the right
Ctrl-E	Move the cursor to the end of the line
Esc-B	Move the cursor back one word
Esc-F	Move the cursor forward one word
Backspace	Move the cursor left, deleting the previous character
Ctrl-D	Delete the character at the present cursor position
Ctrl-U	Delete text up to the cursor
Ctrl-K	Delete text after the cursor
Ctrl-A	Move the cursor to the beginning of the line
Esc-D	Delete remainder of word
Ctrl-W	Delete word up to the cursor
Ctrl-P	Get prior command history
Ctrl-N	Get next command history
Up cursor key	Review command history one at a time
Down cursor key	View next command until reaching the current command
Ctrl-T	Transpose current and previous characters

2 Startup OLT Product

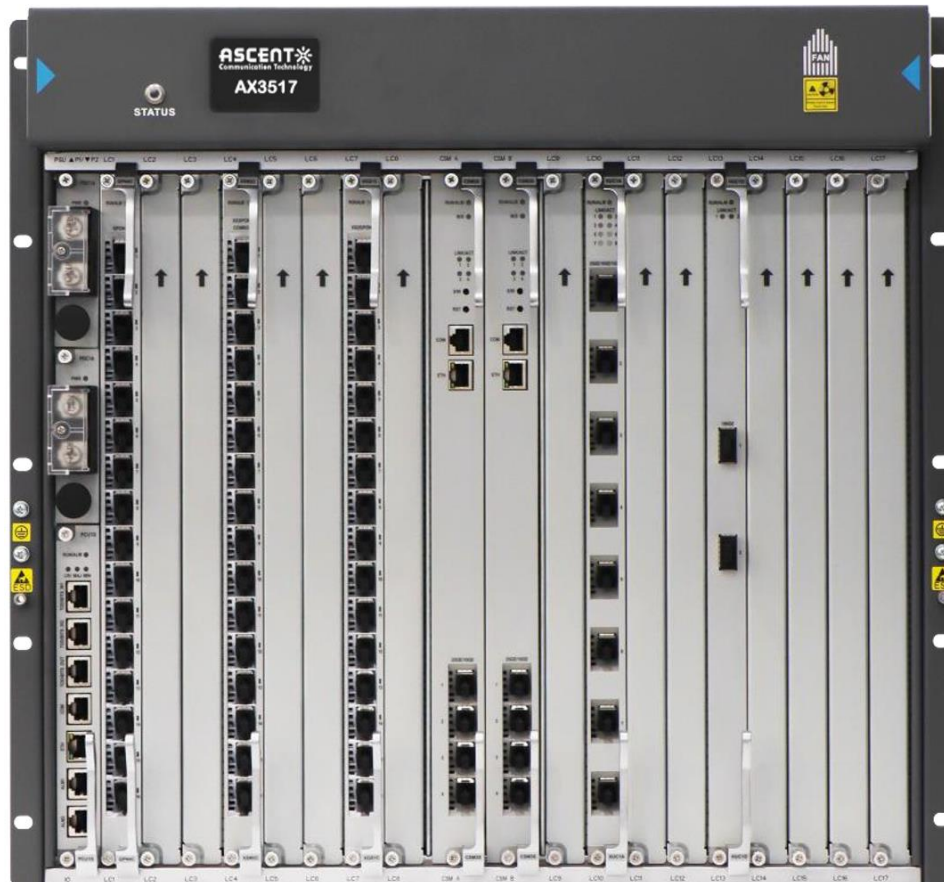
This chapter describes AX3517/AX3515/AX3508/AX3502 startup procedures including other pre-requisite configuration tasks.

The tasks involved in starting up the AX3517/AX3515/AX3508/AX3502 system include:

- System Interface Introduction
- Basic business configuration

2.1 AX3500 Series Product Introduction to System Interface

AX3500 series product adopts frame design. The user side supports 17 service slots. The network side provides 8 * 25GE / 10GE / GE interface (CSM3S), N * 8 * 25GE / 10GE / GE (XUC1A) and N * 2 * 100GE (HUC1D) to ensure non-blocking transmission of services. The specific deployment diagram is shown in below figure:



2.2 Configure Basic Data Service Concept

Before configuring AX3517/AX3515/AX3508/AX3502, pay attention to the following concepts:

- Inband and out-of-band management
- ONU Registration

2.2.1 In-Band and Out-of-Band Management

Through in-band management, the administrator can remotely manage the AX3517/AX3515/AX3508/AX3502 system. In-band management can be operated through the uplink port of AX3517/AX3515/AX3508/AX3502.

Out of band management can be operated locally through AX3517/AX3515/AX3508/AX3502 management port (10 / 100M). For network security, the port is in a demilitarized zone (DMZ).

2.2.2 ONU Registration

AX3517/AX3515/AX3508/AX3502 supports different types of PON cards. Each GPON port (hereinafter referred to as PON port) can connect up to 128 onus, and each xgpon / xgspn port can connect up to 256 onus. The GPON system supports multiple authentication modes (SN authentication, Sn & password authentication, password authentication and disable authentication). AX3517/AX3515/AX3508/AX3502 assigns corresponding ONU IDs to onus that have passed the authentication.



Note: In order to facilitate ONU maintenance related to VLAN allocation, Sn authentication is recommended.

By default, OLT enables Sn authentication mode.

The following command ID is used to configure the ONU binding with the ONU:

```
AX3517# slot 1
```

```
AX3517(Slot-1)#
```

```
AX3517(Slot-1)#interface gpon-olt 1/1
```

```
AX3517(Slot-1/if-gpon-olt-1/1)# ont 1
```

```
AX3517(Slot-1/if-gpon-ont-1/1/1)# sn GPON01234567 type <onu type>
```

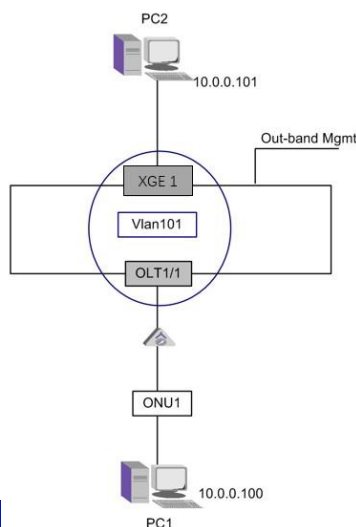
2.3 Configure Basic Data Service Instance

2.3.1 Application Description

VLAN planning should be performed before configuring AX3517/AX3515/AX3508/AX3502 as an L2 switch. In the following topology example, the system VLAN ID is 101. The uplink AX3517/AX3515/AX3508/AX3502 GE port and the downlink AX3517/AX3515/AX3508/AX3502 OLT port are members of system VLAN 101.

In the following example, the PCs connected to the ONU and AX3517/AX3515/AX3508/AX3502 receive their IP addresses statically. However, in a typical network configuration, the PCs can also be assigned IP addresses dynamically via DHCP or PPPoE.

2.3.2 Opology Instance



The simplified topology shown above is used to describe L2 Switch configuration. PC1 is connected to the OLT 1/1 via an ONU. PC2 is connected to the uplink port GE1.

In this example, the ONU VLAN mode is "tag mode", the ONU is the uplink untag message plus VLAN tag 101, and the downlink stripping VLAN tag 101 (the ONU configuration is not within the scope of this document, please refer to the relevant manuals of ONU for details).

In order to ensure the normal operation of layer 2 services of AX3517/AX3515/AX3508/AX3502, the connection between two PCs can be checked by Ping PC2 (or PC2 Ping PC1) from PC1.

2.3.3 Configuration Tasks

The list of tasks related to AX3517/AX3515/AX3508/AX3502 configuration basic data service is as follows:

- Configure uplink port and VLAN
- Configure ONU registration
- Configure ONU data flow service
- Configure VLAN translation
- Connection test

Next, take the topology in Opology Instance figure as an example to introduce the detailed steps of each task.

2.3.4 Configure Uplink Port and VLAN

- Configure port enable

```
AX3517# configure
```

```
AX3517(CONFIG)# l2
```

```
AX3517(CONFIG/L2)# port
```

```
AX3517(CONFIG/L2/PORT)# enable xge 1
```

- Check the port status

```
AX3517(CONFIG/L2/PORT)# show port xge 1
```

```
Port Admin per CfgSpeed CfgDup CfgFlow ActSpeed ActDup ActFlow Orient
```

```
XGE 1 Unlock Up Auto Auto Auto 10000M Full Off Network
```



Note: Link status "up" indicates that the port link communication has been established.

- Create VLAN 101.

```
AX3517# configure
```

```
AX3517(CONFIG)# l2
```


```
AX3517(CONFIG/L2)# vlan
```


```
AX3517(CONFIG/L2/VLAN)# vid 101 name 101 mode full-bridge
```

- Add xge1 as a member of VLAN 101.
AX3517(CONFIG/L2/VLAN)# interface xge 1 vid 101 untag
- Check the configuration information of VLAN 101.
AX3517(CONFIG/L2/VLAN)# show 101
- Return to the configure terminal command mode.
AX3517(CONFIG/L2/VLAN)# exit
AX3517(CONFIG/L2)# exit
AX3517(CONFIG)#

2.3.5 Configure ONU Registration


ONUs connected to the same PON port can be bound to any ONU ID.

- Enter the line card command mode.
AX3517# slot 1
AX3517(slot-1)#
- Enter the OLT port configuration command mode.
AX3517(slot-1)# interface gpon-olt 1/1
AX3517(Slot-1/if-gpon-olt-1/1)#
- Assign ONU ID 1 to ONU and enter ONU configuration mode.
AX3517(Slot-1/if-gpon-olt-1/1) ont 1
AX3517(Slot-1/if-gpon-olt-1/1/1)#
- From the configuration command mode of ONU, bind the SN of onu1 with the ONU ID.
 **Note:** The SN of the ONU can be found on the label on the bottom cover of the ONU.
AX3517(Slot-1/if-gpon-ont-1/1/1)# sn GPON01234567 type <onu type>

- Enter the exit command to return to the line card OLT command mode.
 **Note:** When the communication link between ONU and OLT is normal, the CLI command `brief show slot < slot ID > ont unbound` can be used to obtain Sn information of unauthenticated ONU.

- Use the following command to check the registration status of ONU on OLT 1 / 1.
AX3517(Slot-1)#brief-show slot 1 ont-info

ONT	SN	Status	Find	Auth	Reason
1/1/1	GPON00062845	offline	auto	snonly	inactive
1/8/1	GPON000626D3	ready	auto	snonly	none

-  **Note:** Status "ready" indicates that ONU has successfully completed registration and authentication.

- View other information of ONU.

```
AX3517(Slot-1)#brief-show slot 1 interface gpon-olt 1/1 ont 1 summary
```

```
AX3517(Slot-1)#brief-show slot 1 interface gpon-olt 1/1 ont 1 brief
```

2.3.6 Configure ONU Data Flow Service

Enter the line card command mode and configure the ONU service flow profile.

AX3517/AX3515/AX3508/AX3502 creates profile 1 by default. In order to more clearly describe the configuration process, this example takes the new profile 2 as an example. See the chapter "GPON configuration" for the specific meaning of the parameters involved.

```
AX3517#slot 1
```

```
AX3517(slot-1)#
```

The following commands configure the DBA description profile to describe the bandwidth mode and parameters of the uplink DBA.

```
AX3517(slot-1)# gpon profile dba id 2 name dba_2 type4 max 1244160
```

The following commands configure the t-cont service business profile and bind the DBA description profile.

```
AX3517(slot-1)# gpon profile flow id 2 1 name flow2 uni-type veip uni_bitmap 0xff upmap-type vlanId 101  
101 pri-bitmap 0xff vport 1
```

The following command is used to bind virtual port and t-cont service business profile.

```
AX3517(slot-1)# gpon profile tcont-bind id 2 v-port 1 name bind_id  
2 vportsvc-id 1 tcont-id 1 tcontsvc-id 2
```

The following commands enter the ONU configuration mode to configure the ONU virtual port.

```
AX3517(slot-1)# interface gpon-olt 1/1
```

```
AX3517(slot-1/if-gpon-olt-1/1)# ont 1
```

```
AX3517(slot-1/if-gpon-ont-1/1/1)# virtual-port 1 port unlock
```

The following command applies the business profile to the ONU.

```
AX3517(slot-1/if-gpon-ont-1/1/1)# service flow-profile 2 tcont-bind-profile 2
```

2.3.7 Configure ONU Data Flow Service

Enter VLAN configuration command mode to configure VLAN translation. Please refer to VLAN translation for specific parameters.

```
AX3517#configure
```

```
AX3517(CONFIG)#l2
```

```
AX3517(CONFIG/L2)#vlan
```

```
AX3517(CONFIG/L2/VLAN)# translate slot 1 port 1 ont 1 virtual-port
```

```
1 svid 101 new-svid 101
```

2.3.8 Connection Test

If you want to confirm whether the service configuration is successful, send the ping command to PC2 in PC1.

3 System Configuration

3.1 In-Band and Out-of-Band Introduction

In-band management allows the administrator to remotely manage AX3517/AX3515/AX3508/AX3502 through ISP network.

AX3517/AX3515/AX3508/AX3502 can use any port connected to it for remote in-band management. The ports used are assigned to specific VLANs according to the prior network planning.

Out of band management is performed locally through the mgmt (Management) port of AX3517/AX3515/AX3508/AX3502. This port can be placed in the isolation zone (DMZ) in the ISP network. AX3517/AX3515/AX3508/AX3502 management port is shown in Terminal Emulation Login Connector of RJ-45 / DB9 RS-232 serial port cable connection figure.

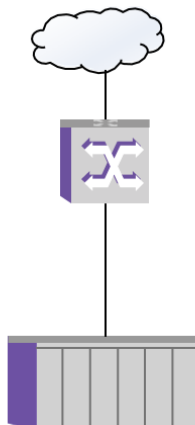


Note: In-band and out-of-band addresses cannot be configured in the same network segment.

3.1.1 In-Band Management Configuration

If you want remote access through the AX3517/AX3515/AX3508/AX3502 uplink port for in-band management, the uplink port must be configured as a VLAN interface.

3.1.1.1 Topology Instance



3.1.1.2 Configuration Requirements

The connection between the management PC and the switch has been configured according to the network planning.

The SVI on the switch has been configured according to the network requirements.

3.1.1.3 Configure Task List

The task list of configuring the in-band management port using SVI is as follows:

- Configuration management VLAN
- Configure management IP address
- Configure in-band management
- View management mode and IP address
- Log in to AX3517/AX3515/AX3508/AX3502 from PC via telnet

Next, take the topology in above figure as an example to introduce the detailed steps of each task.

3.1.1.4 Configure Management VLAN

- Create and manage VLANs according to network planning. In this example, the VLAN ID is 400.

```
AX3517(CONFIG/L2/VLAN)# vid 400 name 400 mode routed
```

- Add port xge4 as a tagged member of VLAN 400.

```
AX3517(CONFIG/L2/VLAN)# interface xge 4 vid 400 tag
```

3.1.1.5 Configure Management IP Address

In this example, the management IP address is 10.1.1.10

```
AX3517(CONFIG/L3)#interface vlan 400:1 ip 10.1.1.10 netmask  
255.255.255.0
```

3.1.1.6 View Management Mode And IP Address

```
AX3517#brief-show interface
```

3.1.1.7 Login From PC via Telnet

- Send ping command from PC to AX3517/AX3515/AX3508/AX3502 and check the connection between PC and AX3517/AX3515/AX3508/AX3502.

- Login AX3517/AX3515/AX3508/AX3502 from PC using telnet.

```
c:\> telnet 10.1.1.10
```

- According to the login prompt, enter the user name and password.

```
10.1.1.10 login: admin Password:
```

```
You are now in the Privileged Admin Mode
```

3.1.2 Out of Band Management Configuration

3.1.2.1 Configuration Instance

For example, configure the out-of-band management IP address as 192.168.7.101 and the gateway as 192.168.7.1.

```
AX3517(IP)#management ip 192.168.7.70 netmask 255.255.255.0
```

This command will change the IP address to 192.168.7.70. Execute anyway? (yes or no)

y

```
AX3517(IP)#route 0.0.0.0 netmask 0.0.0.0 gateway 192.168.7.1
```

3.1.2.2 Management Session Timeout

On AX3517/AX3515/AX3508/AX3502, both in-band and out-of-band management have default management timeout. CLI timeout is configurable.

Enter the following cli command to set the timeout value:

```
AX3517# access idle-timeout <60..100000>.
```

3.2 Configure Basic System Information

This section describes the steps to configure the following basic system parameters:

- Contact information
- System location
- System name
- System clock

Configuration Instances

- Display basic system information.

```
AX3517# system
```

```
contact - System contact
```

```
location - System location
```

```
name - System name, system name
```

```
is displayed in prompt
```

- Set AX3517/AX3515/AX3508/AX3502 host name.

```
AX3517# system name AX3517/AX3515/AX3508/AX3502-1
```

```
AX3517/AX3515/AX3508/AX3502#
```

- Set the AX3517/AX3515/AX3508/AX3502 cli timeout.

```
AX3517# access idle-timeout <60...100000>
```

- Set AX3517/AX3515/AX3508/AX3502 cli system time.

```
AX3517# time <yyyy/mm/dd/HH/MM/SS>
```

```
AX3517# timezone <gmt-12,...gmt-0,...gmt+13>.
```



Note: After the system is restarted, the system clock does not need to be reconfigured, and the internal power supply can keep the clock running for a period of time.

- Save the configuration.

```
AX3517#save config
```

3.3 SNMP Initialization Configuration

Network management system (NMS) communicates with NE through simple network management protocol (SNMP) and supports various management functions. Each management NE is configured as an SNMP agent and supports SNMPv2. Each network element SNMP agent maintains a persistent management information base (MIB), which contains node level function, fault and performance management information. The network element SNMP agent also controls the management information flow between the management server and the node.

3.3.1 Application Description

In this example, Numax Cloud 4000 is an SNMP server for managing AX3517/AX3515/AX3508/AX3502. The topology is the same as figure Topology Instance, where the SNMP server is configured as a trap receiver.

3.3.2 Configuration Requirements

- The Numax 4000 is installed on the SNMP server.
- The layer 3 switch interface connected to SNMP server and AX3517/AX3515/AX3508/AX3502 has been configured.

3.3.3 Configure Task List

The task list of configuring SNMP on AX3517/AX3515/AX3508/AX3502 system is as follows:

- Configure In-Band Management
- Configure SNMP

Next, take the topology in Topology Instance as an example to introduce the detailed steps of each task.

3.3.4 Configure In-Band Management

Configure AX3517/AX3515/AX3508/AX3502 in-band management. For details, see [in-band management configuration](#).

3.3.5 Configure SNMP

- Configuration AX3517/AX3515/AX3508/AX3502 SNMP Community.

AX3517/AX3515/AX3508/AX3502 supports two communities, one is read-only community, and the default is "public". The other is read-write community, which defaults to "xpress". The community

string consists of up to 31 numbers and letters. Ensure that the community string configuration between AX3517/AX3515/AX3508/AX3502 and the server matches. The following commands can



to configure the community string. These commands will override the default community

Note: In the following commands, "mypublic" and "myprivate" can be replaced by the actual community string.

```
AX3517# snmp community "mypublic" read-only
```

```
AX3517# snmp community "myprivate" read-write
```

- Configure the trap receiver (here 192.168.103.100 is used as the IP address of the SNMP server)

```
AX3517# snmp trap-destination 192.168.103.100 community myprivate
```



Note: You can also configure the trap receiver on the SNMP server. For details, please refer to the network management operation manual.

3.3.6 Configure SNMPv3

SNMPv3 inherits from SNMPv2 and provides more advanced security features, including authentication, encryption and access control

Authentication and encryption: SNMPv3 introduces User Security Model (USM) and View-based Access Control model (VACM), which support data encryption and user authentication to ensure the security of management information. This feature enables SNMPv3 to better protect network management information against unauthorized access and potential attacks.

User management functions: SNMPv3 supports more user management functions, including user authentication, user group management, user password policies, and user activity tracking. These capabilities provide more fine-grained access control and help to implement stricter security policies.

USM (User-Based Security Model)

USM introduces the concept of user name and group, authentication and encryption functions can be set. Authentication is used to verify the legitimacy of the message sender to avoid the access of illegal users. Encryption, on the other hand, encrypts the packets transmitted between the NMS and the Agent to avoid eavesdropping.

The combination of functions with or without authentication and with or without encryption can provide higher security for the communication between NMS and agents.

VACM (View-based Access Control Model)

VACM technology defines five elements: group, security level, context, MIB view and access policy. These elements simultaneously decide whether a user has access rights or not, and only users with access rights can manage the operation object.

Different groups can be defined on the same SNMP entity, the group is bound to the MIB view, and multiple users can be defined within the group. When a user name is used, only objects defined by the MIB view can be accessed.

1. Configure MIB view.

```
AX3517#snmpv3 mib-view <view-name> <include|exclude>
```

```
<subtree-oid> mask <mask-value>
```



Note: Mask is a hexadecimal mask, such as FF8.

SNMP view: It allows you to define what information a user can access, effectively limiting access to devices on the network and preventing unauthorized parties from reading/writing data.

2. Configure user group.

```
AX3517#snmpv3 group 1 <noauth|authentication|privacy> read-view 1 write-view 2 notify-view 3.
```



Note: Noauth means no authentication, authentication means only authentication, and privacy means authentication and encryption

SNMP group: Defines the user's access type (read-only or read/write) and security type, which specifies the level of security when interacting with the device

3. Configure snmpv3 user , binding group1, Set authentication mode, authentication password, encryption mode, encryption password.

```
AX3517#snmpv3 usm-user <user-name> group 1 auth-mode sha 1234567 privacy-mode  
<des|aes128> 12345678
```

3.4 Configure SNTP

This section describes configuring the SNTP client to obtain clock synchronization from the SNTP server through the SNTP protocol. Synchronization messages interact through in-band / out-of-band management interfaces. CLI configuration commands are as follows:

- Configure SNTP server address. AX3517/AX3515/AX3508/AX3502 supports up to three server addresses.

```
AX3517#sntp server <IP Address>
```

```
AX3517#sntp option <enable|disable>
```

- Configure SNTP related parameters.

```
AX3517#sntp [poll-interval <Interval>]
```

Key parameters are described in below figure.

Field	Value Range	Default Values	Explain
Poll-interval	60-65535	1200	Optional, synchronization interval, in seconds.
Sync	NA	NA	Optional, manual synchronization.
Ptype	Ntp sntp	Sntp	Protocol type

3.5 Alarm

This section describes the configuration and display of system alarm:

View the current alarm.

AX3517#brief-show alarm

Configure the alarm LED status, and the user can set the alarm led on / off as required.

AX3517#alarm alarm-led-control <critical|major|minor> <on|off>

The description of alarm list is shown in below table

Alarm Description		Alarm description		Level	Cause	Resolution
Module Mismatch	Type	Module mismatch	type	Major	The currently inserted module type does not match the virtual dominated module type	The virtual module is de dominated or cleared after the currently inserted module is pulled out or reset
Module unrecognized		Module not recognized		Major	Unrecognized module due to module insertion failure	The module is later recognized or cleared after the module is pulled out or reset
Module failed to come up		The module cannot start normally		Major	Due to module failure, although the module is recognized by the node, the module cannot start to provide services normally	After the module starts the service or the module is pulled out or reset, it is cleared
Assigned module removal		Module pulled out		Major	The normally matched module is pulled out	The module is reinserted or cleared after the virtual module is de dominated
Standby removal	CSM	Standby CSM module pulled out		Major	The standby CSM module is pulled out	Clear after the standby CSM module is plugged back in
Standby CSM is running a higher version image		A higher version of software is running on the standby CSM		Minor	A higher version of software is running on the standby CSM	CSM switching or clearing after standby CSM is pulled out or reset
Standby CSM is running a lower version image		An earlier version of the software is running on the standby CSM		Major	An earlier version of the software is running on the standby CSM	CSM switching or clearing after standby CSM is pulled out or reset
Module image version mismatch		Module software version mismatch		Minor	The software version running in the module is different from that in the node version file	Clear after the module is pulled out or reset
Hearbeat signal failed between two redundancy CSM modules		Heartbeat signal failure between primary and standby CSMS		Major	Heartbeat signal failure between primary and standby CSMS	The standby CSM is pulled out or cleared after the heartbeat signal is restored
Protection uplink on active CSM is down		The uplinkprotection link of the main CSM is disconnected		Critical	The uplink protection link of the main CSM is disconnected	After the main link is removed or the CSM is removed, the CSM is reset with the main link

Alarm Description	Alarm description	Level	Cause	Resolution
Protection uplink on standby CSM is down	The uplink protection link of the standby CSM is disconnected	Major	The uplink protection link of the standby CSM is disconnected	During CSM switching, the standby CSM is pulled out or reset, and the uplink protection link of the standby CSM is cleared after recovery
Image file failed to be downloaded into module	Module download software failed	Minor	Module download software failed	The module is unplugged or cleared after subsequent successful downloads
Version file is missing	Version file not found	Major	There is no version file in the shelf	Clear after software version is retrieved
Module ambient temperature exceeds the warning threshold	The temperature around the module exceeds the alarm temperature threshold	Minor	The temperature around the module is equal to or higher than the alarm temperature threshold (T1)	Module reset, unplug or the temperature around the module is lower than the alarm temperature, or the temperature around the module is equal to or higher than the short-time tolerance temperature threshold
Module ambient temperature exceeds the short-time tolerance threshold	The temperature around the module exceeds the short-time tolerance temperature threshold	Major	The temperature around the module is equal to or higher than the short-time tolerance temperature threshold (T2)	Module reset, pull out or the temperature around the module is lower than the short-time tolerance temperature threshold, or the temperature around the module is higher than the shutdown temperature threshold
Environmental temperature cross the high-temperature threshold	The temperature around the module exceeds the shutdown temperature threshold	Major	The temperature around the module is equal to or higher than the shutdown temperature threshold (T3)	Clear after module reset or unplug
Environmental temperature cross the high-temperature threshold	The ambient temperature exceeds the high temperature threshold	Critical	The detected ambient temperature exceeds the high temperature threshold	Reset the node and clear it after the next detected ambient temperature is 3 ° C lower than the high temperature threshold
Environmental temperature cross the low-temperature threshold	The ambient temperature exceeds the low temperature threshold	Critical	The detected ambient temperature exceeds the low temperature threshold	The node is reset and cleared after the next detected ambient temperature is 3 ° C higher than the low temperature threshold
Fan Tray absent	Fan disc not in position	Major	Fan disc not in position	Clear after the fan disk is inserted
One or two FANs fails working	One or both fans stop working	Minor	One or both fans stop working	Pull out the fan disk, all fans work normally or clear after more than two fans stop working

Alarm Description	Alarm description	Level	Cause	Resolution
More than two FANs fail working	More than two fans stop working	Major	More than two fans stop working	When the fan disk is pulled out, all fans work normally or only one or two fans stop working
Time server is down	Time Server Disconnected	Minor	Responses from all configured SNTP servers were not received during the polling cycle	Clear after receiving the response from any SNTP server in the next polling cycle
The threshold of CPU occupancy in CSM is crossed	The CPU share of the main CSM exceeds the threshold	Minor	The CPU share of the main CSM exceeds the threshold	In the following polling, clear after the CPU occupancy is lower than the overload threshold
The threshold of Memory occupancy in CSM is crossed	The memory occupancy of the main CSM exceeds the threshold	Minor	The memory occupancy of the main CSM exceeds the threshold	Clear after the memory occupancy is below the overload threshold in the following polling
The threshold of 15min CPU occupancy is crossed	15 minute CPU occupancy exceeds the threshold	Minor	The 15 minute CPU occupancy of the module exceeds the threshold	The module resets or clears after the CPU occupancy is lower than the overload threshold in the following polling
-48VDC input is abnormal	-48V DC power input abnormal	Major	-DC under voltage or over-voltage input 48V	-48V DC power input returns to normal
3.3VDC power output is abnormal	Abnormal output of 3.3V DC power supply	Major	3.3V DC power output overvoltage, undervoltage or overcurrent	3.3V DC power output returns to normal
Ringer power output is abnormal	Abnormal output of bell current power supply	Major	Output undervoltage or overcurrent of bell current power supply	The bell current power output returns to normal
Power output is abnormal	Abnormal power output	Critical	DC power output overvoltage, undervoltage or overcurrent	DC power output returns to normal
CSM XGE down	Uplink disconnection of CSM XGE port	Major	The operation status of the uplink port of CSM XGE port is "disconnected"	The uplink working state of CSM XGE port changes to "normal" or the management state of uplink port changes to "locked"
CSM uplink down	CSM IU uplink board uplink disconnection	Major	The operation status of the uplink port of the CSM IU uplink board is "disconnected"	The working state of the uplink of the CSM IU uplink becomes "normal" or the management state of the uplink port becomes "locked"
CSM uplink down	CSM uplink disconnection	Major	The operation status of CSM uplink port is "disconnected"	The working state of CSM uplink changes to "normal" or the management state of uplink port changes to "locked"

Alarm Description	Alarm description	Level	Cause	Resolution
Trunk work abnormal	Trunk works abnormally	Major	<p>1. The switch router port at the opposite end of the link aggregation may work abnormally. Or,</p> <p>2. The cable used for this link aggregation between the device and the opposite end switch router may be damaged.</p>	The actual speed, duplex mode, or flow control of the active trunk member port are consistent
Trunk down	Trunk status down	Major	The running state of CSM trunk is "off"	The working state of CSM trunk changes to "normal" or the management state of trunk changes to "locked"
XGE optical transceiver TX power high alarm	XGE optical module sends high optical power alarm	Major	The optical power transmitted by XGE optical module is higher than the set threshold	The optical power transmitted by XGE optical module is lower than 5% of the set threshold
XGE optical transceiver TX power low alarm	XGE optical module sends low optical power alarm	Major	The optical power transmitted by XGE optical module is lower than the set threshold	XGE optical module sends optical power higher than 5% of the set threshold
XGE optical transceiver supply voltage high alarm	XGE optical module transceiver high voltage alarm	Major	XGE optical module transceiver voltage above set threshold	XGE optical module transceiver voltage is lower than 5% of the set threshold
XGE optical transceiver supply voltage low alarm	XGE optical module transceiver low voltage alarm	Major	XGE optical module transceiver voltage below the set threshold	XGE optical module transceiver voltage is higher than 5% of the set threshold
XGE optical transceiver bias current high alarm	XGE optical module transceiver bias high alarm	Major	XGE optical module transceiver bias is higher than the set threshold	The bias current of XGE optical module transceiver is lower than 5% of the set threshold
XGE optical transceiver bias current low alarm	XGE optical module transceiver bias low alarm	Major	The bias current of XGE optical module transceiver is lower than the set threshold	The bias current of XGE optical module transceiver is higher than 5% of the set threshold
XGE optical transceiver temperature high alarm	XGE optical module transceiver high temperature alarm	Major	XGE optical module transceiver temperature above the set threshold	The XGE optical module transceiver temperature is below 5% of the set threshold
XGE optical transceiver temperature low alarm	Low temperature alarm of XGE optical module transceiver	Major	The XGE optical module transceiver temperature is below the set threshold	The XGE optical module transceiver temperature is higher than 5% of the set threshold
XGE optical transceiver TX power high warning	XGE optical module sends high optical power warning	Warning	The optical power transmitted by XGE optical module is higher than the set threshold	The optical power transmitted by XGE optical module is lower than 5% of the set threshold
XGE optical transceiver TX power low warning	XGE optical module sends low optical power warning	Warning	The optical power transmitted by XGE optical module is lower than the set threshold	XGE optical module sends optical power higher than 5% of the set threshold

Alarm Description	Alarm description	Level	Cause	Resolution
XGE optical transceiver supply voltage high warning	XGE optical module transceiver high voltage warning	Warning	XGE optical module transceiver voltage above set threshold	XGE optical module transceiver voltage is lower than 5% of the set threshold
XGE optical transceiver supply voltage low warning	XGE optical module transceiver low voltage warning	Warning	XGE optical module transceiver voltage below the set threshold	XGE optical module transceiver voltage is higher than 5% of the set threshold
XGE optical transceiver bias current high warning	XGE optical module transceiver bias high warning	Warning	XGE optical module transceiver bias is higher than the set threshold	The bias current of XGE optical module transceiver is lower than 5% of the set threshold
XGE optical transceiver bias current low warning	XGE optical module transceiver low bias warning	Warning	The bias current of XGE optical module transceiver is lower than the set threshold	The bias current of XGE optical module transceiver is higher than 5% of the set threshold
XGE optical transceiver temperature high warning	XGE optical module transceiver high temperature warning	Warning	XGE optical module transceiver temperature above the set threshold	The XGE optical module transceiver temperature is below 5% of the set threshold
XGE optical transceiver temperature low warning	XGE optical module transceiver low temperature warning	Warning	The XGE optical module transceiver temperature is below the set threshold	The XGE optical module transceiver temperature is higher than 5% of the set threshold
XGE optical transceiver Rx power high alarm	XGE optical module transceiver receives high power alarm	Major	The received optical power of XGE optical module is higher than the set threshold	The received optical power of XGE optical module is lower than 5% of the set threshold
XGE optical transceiver Rx power low alarm	XGE optical module transceiver receives low power alarm	Major	The received optical power of XGE optical module is lower than the set threshold	The received optical power of XGE optical module is higher than 5% of the set threshold
XGE optical transceiver Rx power high warning	XGE optical module transceiver receives high power warning	Warning	The received optical power of XGE optical module is higher than the set threshold	The received optical power of XGE optical module is lower than 5% of the set threshold
XGE optical transceiver Rx power low warning	XGE optical module transceiver receives low power warning	Warning	The received optical power of XGE optical module is lower than the set threshold	The received optical power of XGE optical module is higher than 5% of the set threshold
ROGUE ONT	Rogue ont	Major	Rogue ont detected under PON	Remove rogue ont
LOSi	ONT LOSi Alarm	Warning	The OLT cannot receive the light of the specified ONU	OLT detects normal ONU illumination

Alarm Description	Alarm Description	Level	Cause	Resolution
SFi	ONU signal failure	Warning	BER (ONU bit error rate) is calculated for each interval t. T is the parameter set by the application. If $BER \geq BER\ SF$ threshold, SFI alerts are sent to the host application. The BER SF threshold is defined as $10-x$, where x is configurable in the range of 3 to 8.	The alarm must be cleared by the host after the ONU is successfully activated
SDi	ONU signal degradation	Warning	BER (ONU bit error rate) is calculated for each interval t. T is the parameter set by the host application. If $BER \geq BER\ SD$ threshold, the SDI alert is sent to the host application. BER SD threshold is $10-x$, where x can be configured in the range of 4 to 9	SD threshold must be higher than SF threshold. When $BER < 10 - (x + 1)$, SDI is cleared.
GTCAi	Gem port packet loss	Warning	Gem port packet loss	ONU successfully launched
ETCAi	Eht port FEC error	Warning	FEC error	
TIWi	The transmission of ONU is disturbed	Warning	This alert is triggered when the average drift of the ONU is detected Predefined threshold exceeded	ONU successfully launched
LOFi	Frame loss of ONU	Warning	This alert is triggered by N consecutive invalid delimiters of the ONU, where n is available through <code>bcmolt_cfg_Set (gpon_ni)</code> API is configured (the default value is 4). When LOFI is detected, the ONU is disabled and a notification is sent to the host application. The alarm is Clear after successfully activating ONU.	ONU successfully launched
MEMi	Message error of ONU	Warning	When an unknown ploam message is received, <code>bcm68620</code> The firmware sends notifications to the host application. This notification includes the ploam message received	

Alarm Description	Alarm description	Level	Cause	Resolution
LOKi	ONU lost synchronization key	Warning	<p>Key exchange process due to request_ The key ploam message failed 3 times without response. The alarm will be cleared and encryption will be received if_ After the key ploam message or the successful ONU activation process.</p> <p>When Loki is detected, the ONU is disabled and a notification is sent to the host application.</p>	ONU successfully launched
LOBi	ONU burst lost	Warning	This alert is triggered by N consecutive invalid delimiters of the ONU, where n is configurable through link configuration.	ONU successfully launched
DOWi	Drift of ONU window	Warning	This alert is triggered when the average drift detected for the ONU exceeds a predefined threshold.	Clear the alarm when the average drift falls below the threshold
LOPCi	XG (s) ploam message missing	Warning	Loss of ploam channel of ONU - when n consecutive times, this alarm is triggered by bcm686xx firmware. There is a lack of ploam message, acknowledgement or continuous mic failure in ONU.	ONU successfully launched
LOOCi	OMCI channel failed	Warning	<p>This alarm is triggered by bcm686xx firmware when OMCI is performed n times in a row</p> <p>Received a packet with MIC error.</p>	ONU successfully launched
LCDGi	Gem channel demarcation lost	Warning	When the gem channel demarcation of ONU is lost	When the gem channel demarcation of ONU is restored
LOAi	ONU protocol acknowledgement frame lost	Warning	The OLT did not receive the uplink confirmation message that the ONU should send	When OLT receives confirmation from ONU
DFi	ONU inactive failed	Major	This alarm is generated when OLT receives three consecutive messages	Activate ONU
RDli	ONU remote defect indication	Warning	When the RDI domain in the ONU is declared, the OLT data received at the ONU is defective.	When the RDI signal of ONU disappears

Alarm Description	Alarm Description	Level	Cause	Resolution
SUFI	ONU startup failed	Warning	OLT receives optical pulse from ONU After that, the ONU ranging failed n times, (n=2)	After the ONU is activated successfully, the alarm is cleared
DGi	Dying gasp received from ONU	Minor	When the OLT receives the dye gasp message from the ONU, it declares the dye gaspi	When OLT receives ploam message during ranging
PEEi	ONU physical device error	Warning	When the OLT receives a pee message from the out	3 seconds after OLT does not receive the pee message from ONU
LOS	Loss of PON optical port signal	Major	No optical receiving port PON	The PON port is cleared after receiving the optical signal or disabling the port
OLT port admin state link down	PON port admin state link down	Warning	PON port Link Down	PON port Link Up

3.6 Node Access Control

This function controls Telnet, SNMP, TFTP, SSH, and FTP access permissions based on IP.

When enabled, only the configured IP range is accessible.

3.6.1 SNMP Access Control

Configuring access permissions

Restricted access to SNMP, configured and enabled only IP 192.168.7.x can access with read-only permissions

```
AX3517(Access)#snmp-host 192.168.7.101 netmask 255.255.255.0
```

```
privilege RO
```

When configured and enabled, only IP 192.168.7.x can be accessed with read and write permissions

```
AX3517(Access)#snmp-host 192.168.7.101 netmask 255.255.255.0
```

```
privilege RW
```



Note: RO/RW mean read-only or read-write.

Enable/disable snmp-host-list

```
AX3517(Access)#snmp-host-list
```

```
enable AX3517(Access)#snmp-host-list disable
```

3.6.2 Telnet Access Control

Telnetv4 access control configuration. Only devices with IP 192.168.7.x can access OLT through telnet after configuration and enabled

```
AX3517(Access)#telnet-host 192.168.7.101 netmask 255.255.255.0
```

Telnetv6 access control configuration. Only devices with IPv6 address 2000::12:101 can access OLT through telnet after configuration and enabling

```
AX3517(Access)#telnet-hostv6 2000::12:101 prefix 128
```

Telnet access control list enable/disable

```
AX3517(Access)#telnet-host-list enable AX3517(Access)#telnet-host-list disable
```

3.6.3 SSH Access Control

SSHv4 access control. Only devices with IP 192.168.7.x can access OLT through ssh after configuration and enabling.

```
AX3517(Access)#ssh-host 192.168.7.101 netmask 255.255.255.0
```

SSHv6 access control, after configuration, only the device with IPv6 address 2000::12:101 can access the OLT through ssh.

```
AX3517(Access)#ssh-hostv6 2000::12:101 prefix 128
```

SSH access control list enable/disable.

```
AX3517(Access)#ssh-host-list enable AX3517(Access)#ssh-host-list disable
```

3.6.4 TFTP Access Control

tftp access control. After configured and enabled, only devices with IP 192.168.7.x can access OLT through tftp

```
AX3517(Access)#tftp-host 192.168.7.101 netmask 255.255.255.0
```

Tftp access control list enable/disable

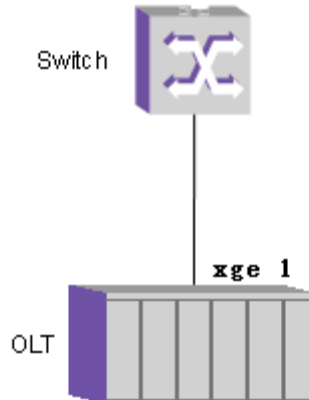
```
AX3517(Access)#tftp-hostt-list enable
```

```
AX3517(Access)#tftp-hostt-list disable
```

3.7 LLDP

OLT can notify other devices of their status by sending Link Layer Discovery Protocol Data Unit (LLDPDU) on the local network. It is a vendor-independent link layer protocol for network topology, troubleshooting, and network management automation.

3.7.1 Topology Instance



3.7.2 Configuration instance

1. Enable LLDP.

```
AX3517#lldp mode enable
```

2. Configure lldp packet sending rate, aging time and other information.

```
AX3517#lldp global tx_interval 30 tx_hold_multi 2 fast_tx 10
```

```
tx_fast_init 1
```

Feld	Data Rnge	Deault Value	Note
tx_interval	30-32768	30	lldp packet delivery interval
tx_hold_multi	2-10	2	lldp aging time
fast_tx	1-3600	1	Fast sending interval time after neighbor update.
tx_fast_init	1-8	4	Number of lldp packets sent quickly after neighbor update.

3. Enable port sends packets carrying the OLT management IP address.

```
AX3517#lldp man-addr-config-tx set interface "xge 1" tx-enable enable
```

4. Set the port LLDP mode.

```
AX3517#lldp port interface "xge 1" admin-status tx_and_rx          tlvs-tx portDesc, sysName trap-en enable
trap-interval 15
```

Field	Data Range	Default Value	Note
admin-status	tx	NA	Set the port management status to send only/Accept only/Send & Accept/neither send nor receive
	rx		
	tx_and_rx		
	disable		
tlvs-tx	portDesc	NA	Tlv parameter. They are port description, system name, system description, and system support capability
	sysName		
	sysDesc		
	sysCap		
trap-interval	5-3600	30	Packet delivery interval



Note: TLV can use "-" or ", " to select multiple parameters simultaneously. E.g. "portDesc,sysName,sysDesc,sysCap", or "sysDesc,sysCap"

5. Disable LLDP.

AX3517#lldp mode disable

3.8 AAA Authentication

Authentication: authenticating a user's identity and available network services Authorization: Open the network service to the user based on the authentication result; Accounting: Record the usage of various network services and provide it to the accounting system.

3.8.1 Authentication Mode

AX3517(aaa)#authen-mode <authen-mode>

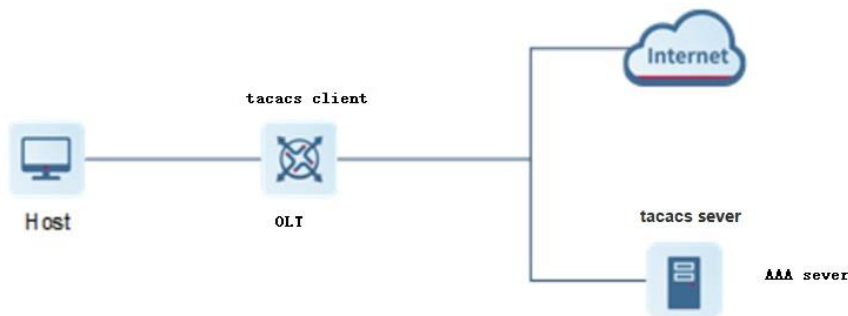
Mode	Descriptions
radius	Radius Authentication.
radius-no-local	Radius Authentication. When the remote login, when the AAA server authentication fails, it will not authenticate with the local existing account and password process, only when the AAA server does not respond, it will verify with the local existing account and password process.
radius-before-local	radius authentication. When the remote login, the priority is to authenticate the account and password on the AAA server. When the AAA server authentication fails, it will check with the local existing account and password, if it passes, it will enter the system.
tacacs	tacacs Authentication.
tacacs-no-local	tacacs authentication. When the remote login, when the AAA server authentication fails, it will not authenticate with the local existing account and password process, only when the AAA server does not respond, it will verify with the local existing account and password process.
tacacs-before-local	tacacs authentication. When the remote login, the priority is to authenticate the account and password on the AAA server. When the AAA server authentication fails, it will check with the local existing account and password, if it passes, it will enter the system.

Mode	Descriptions
local	Local authentication, when the remote login, authentication is not through the AAA server, but based on the existing local account password to verify.

3.8.2 Radius Certification

More than one RADIUS server is usually deployed in a large network. The first purpose of this is that in the case of a server failure, it will not affect the user access. The second is to load balance between multiple servers when a large number of users access, a single server's resources will not be exhausted. When more than one server is configured in the RADIUS server template, the RADIUS client can select the RADIUS server according to the primary and secondary algorithm or load sharing algorithm when sending packets to the server. Therefore, this device supports the configuration of three radius servers.

3.8.2.1 Topology Instance Topology Instance



RADIUS is a protocol of C/S structure, its client is NAS (Net Access Server) server initially, any computer running RADIUS client software can become a RADIUS client.

3.8.2.2 Configuration Instance

- Configure the radius server and the shared secret.

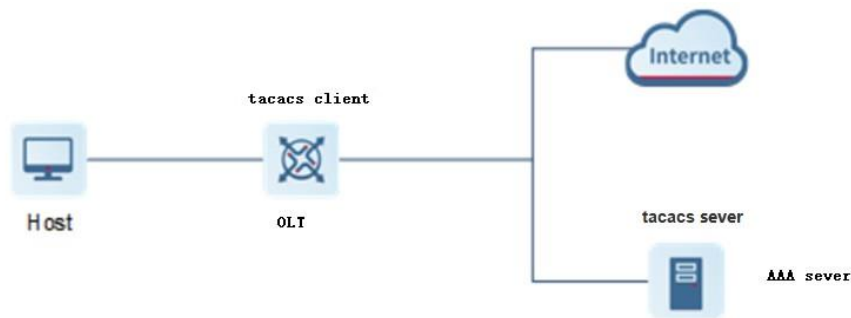

```
AX3517(aaa)#radius server primary ip 10.10.10.1 share-secert radius1
AX3517(aaa)#radius server secondary ip 10.10.10.2 share-secert radiuAX3502
AX3517(aaa)#radius server tertiary ip 10.10.10.3 share-secert radius3
```
- Enable device radius authentication.


```
AX3517(aaa)#authen-mode radius
```

3.8.3 TACACS+ Certification

Like RADIUS, this device also supports the configuration of three TACACS+ servers to realize the primary and secondary mechanism and load sharing.

3.8.3.1 Topology Instance



TACACS allows clients to accept a username and password and send it to a TACACS authentication server, commonly known as the TACACS daemon (or simply TACACSD), which is typically a program running on the host computer. The host will decide whether to accept or reject the request and send back a response

3.8.3.2 Configuration Instance

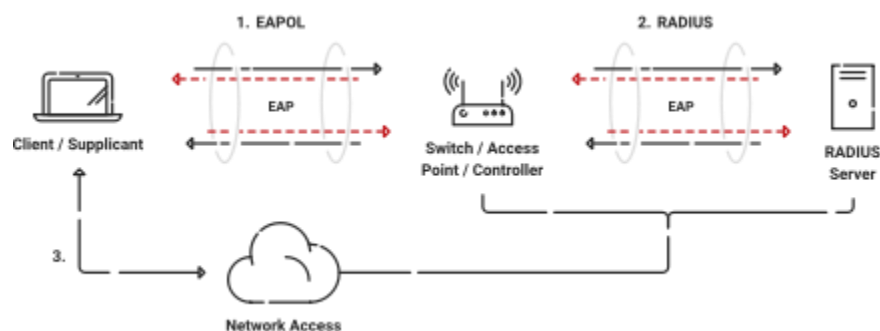
1. Configure the tacacs server and the shared secret
`AX3517(aaa)#tacacs server primary ip 10.10.10.1 share-secret tacacs1`
`AX3517(aaa)#tacacs server secondary ip 10.10.10.2 share-secret tacacs2`
2. `AX3517(aaa)#tacacs server tertiary ip 10.10.10.3 share-secret tacacs3`
3. Enable tacacs authentication of the device
`AX3517(aaa)#authen-mode tacacs`

3.9 802.1x

3.9.1 Introduction

The 802.1x protocol is a client/server-based access control and authentication protocol. It can restrict unauthorized users/devices from accessing the LAN/WLAN through the access port. Before accessing various services provided by the switch or LAN, 802.1x authenticates the users/devices connected to the ONU. Before authentication is successful, only EAPOL (Extensible Authentication Protocol over LAN) data is allowed through the port to which the device is connected. After authentication is successful, normal data can pass smoothly through the Ethernet port.

3.9.2 Topology Instance



The components of the 802.1x system are:

- **Client:** The client is typically a user terminal device. The client must support the Extensible Authentication Protocol over LANs (EAPoL) and install 802.1x client software, enabling users to initiate 802.1x authentication by launching the client software.
- **Access Device:** The access device is typically a network device that supports the 802.1x protocol. It provides the port for the client to access the LAN. This port can be a physical port or a logical port.
- **Authentication Server:** The authentication server is used to authenticate, authorize, and account for users. It is usually a RADIUS server.

3.9.2.1 Authentication Server Configuration

The authentication server is typically a RADIUS server. This OLT can be configured with up to 3 authentication servers.

```
AX3517(aaa)#radius server primary ip 10.10.10.1 share-secert radius1
```

```
AX3517(aaa)#radius server secondary ip 10.10.10.2 share-secert radiuAX3502
```

```
AX3517(aaa)#radius server tertiary ip 10.10.10.3 share-secert radius3
```

3.9.2.2 Enable/Disable 802.1x Authentication Feature

- Enable/disable the 802.1x feature for a specific VLAN

```
AX3517(aaa)#802dot1x vid 101 enable AX3517(aaa)#802dot1x vid 101 disable
```

All related authenticated devices will become unauthenticated when disable his vlan.

Are you sure to disable (y/n)?y

When the 802.1x feature is disabled, all authenticated devices will be disconnected.

- Query 802.1x VLAN.

```
AX3517(aaa)#show 802dot1x vid
```

3.9.2.3 802.1x Timeout

Configure Timeout Parameters.

```
AX3517(aaa)#802dt1x timeout [tx-period <tx-period>] [re-auth-max
```

```
<re-auth-max>][re-auth-period<re-auth-period>][quiet-period<quiet- period>][ handshake-  
period<handshake-period>]
```


Parameter	Descriptions
tx-period	The timeout for no response from the authenticated device, ranging from 1 to 65535 seconds, default is 30s.
re-auth-max	Maximum number of request retransmissions, ranging from 1 to 100, default is 2.
re-auth-period	Interval for re-authentication, ranging from 0 to 65535 minutes, default is 60 minutes. A value of 0 means no re-authentication will occur.
quiet-period	The period after authentication failure before starting the next authentication process. Ranges from 0 to 65535 seconds, default is 60s.

3.9.2.4 Query 802.1x Timeout Parameters

```
AX3517(aaa)#show 802dot1x timeout
```

```
txPeriod : 30s
```

```
reAuthMax : 2
```

```
reAuthPeriod : 60m
```

```
quietPeriod : 60s
```

```
handshakePeriod : 60s
```

3.9.3 MAC Address Control

Allows users to manually add the MAC information of authenticated devices. Once MAC address restriction is enabled, devices without added information will be prohibited from authentication.

- Manually add device MAC information.

```
AX3517(aaa)#device slot 1 pon-port 2 ont 3 vport 4 mac
```

```
00:00:11:22:33:44
```

Add device information successfully.

- Enable/Disable MAC Control.

```
AX3517(aaa)#802dot1x mac-control enable
```

Enable the configuration will disconnect all authenticated devices. Are you

sure to enable (y/n)?y

Set success.

```
AX3517(aaa)#802dot1x#mac-control disable
```

Disable the configuration will erase all added devices info. Are you sure to

disable (y/n)?y

Set success.

3.9.4 Query 802.1x Information

- Query MAC Address Control

```
AX3517(aaa)#show 802dot1x mac-control
```

```
mac control : enable
```

- Query successfully authenticated 802.1x devices that are not online (including devices with MAC address restrictions):

```
AX3517(aaa)#show 802dot1x unauth-dev
```

```
Total Device Count    1
```

```
Virtual Port   MAC Address   S-VID
```

```
-----
```

```
- 1/2/3/4      00:00:11:22:33:44      0
```

- Query information of successfully authenticated devices:

```
AX3517(aaa)#show 802dot1x auth-dev
```

```
Total Device Count    1
```

```
Virtual Port   MAC Address   S-VID
```

```
-----
```

```
1/2/3/3       00:00:02:01:01:02      1050
```

4 L2 Configuration

AX3517/AX3515/AX3508/AX3502 is suitable for various network applications. This chapter describes the steps of configuring AX3517/AX3515/AX3508/AX3502 system according to specific network requirements. This chapter describes the following basic AX3517/AX3515/AX3508/AX3502 configurations:

- Port Properties
- MAC Address Table
- Link Aggregation
- VLAN
- Port Mirroring
- RSTP
- MSTP
- Relay options
- Loop Detection

4.1 SVI Concept

AX3517/AX3515/AX3508/AX3502 10 Gigabit-Ethernet (XGE) ports, Link Aggregation ports, Passive Optical Network (PON) ports or arrange of interfaces can be configured as Layer2 ports.

- XGE ports are switch ports associated with physical ports on the AX3517/AX3515/AX3508/AX3502
- Link Aggregation ports are composed of one or more aggregated GE ports
- IS ports are downlink XGE ports associated to OLT ports.



Note: For PON port configuration, refer to OLT Management.

4.1.1 Administrative Status

The XGE port can be turned on or off by setting the management status of the port. By default, XGE port management status is off.

Use the CLI command `enable` to change the management status of the port to on,

and use the CLI command `disable` to change the management status of the port to off.

```
AX3517(CONFIG/L2/PORT)#enable interface xge 1
```

```
AX3517(CONFIG/L2/PORT)#disable interface xge 1
```

4.1.2 Link Status

The default link state of the XGE port is up.

According to the uplink or downlink status of the port, the link status will change according to the following rules:

AX3517/AX3515/AX3508/AX3502 uplink XGE port: if a physical connection is established with the active node and the management status is on, the link status is up.

```
AX3517(CONFIG/L2/PORT)#show port interface xge 1
```

Port	Admin	Oper	CfgSpeed	CfgDup	CfgFlow	ActSpeed	ActDup	ActFlow	Orient
XGE 1	Unlock	Up	Auto	Auto	Auto	1000M	Full	Off	Network

4.1.3 Self Negotiation and Rate Duplex

AX3517/AX3515/AX3508/AX3502 supports the automatic negotiation function of uplink XGE port. When the self duplex mode and the self duplex mode can be set to the highest level at both ends.

In order to make the self negotiation work normally, the remote device should also have this function. Self negotiation is enabled by default.

```
AX3517(CONFIG/L2/PORT)#speed interface xge 1
```

```
AX3517(CONFIG/L2/PORT)#speed interface xge 1 10GEfon
```

4.1.4 Flow Control

AX3517/AX3515/AX3508/AX3502 provides flow control in both receiving and transmitting directions. In order to make the flow control function normal, the remote equipment should also have this function. Flow control is on by default. Please refer to self negotiation and rate duplex for configuration.

4.1.5 Storm Control

AX3517/AX3515/AX3508/AX3502 provides three types of service storm control: broadcast, unknown multicast and unknown unicast. By setting the threshold of each packet type, data storm can be prevented. Threshold indicates the number of packets passing through the port per second, which is a part of the total available bandwidth of the port. When the threshold is exceeded, the packet is discarded.

When the threshold of a packet type is set to zero, all packets of that type are discarded.

```
AX3517#configure
```

```
AX3517(CONFIG)#security
```

```
AX3517(CONFIG/Security)# storm-control<bclimit|dlf-limit|mclimit>interface xge 1 <bandwidth-Rate,Rate in kbits,the default value is 2000 >
```

4.1.6 User Isolation

AX3517/AX3515/AX3508/AX3502 supports user isolation configuration, which is a global configuration command.

- Open port isolation: users cannot communicate with each other under the same PON port or different PON ports.
- Close port isolation: users can communicate with each other under the same PON port or different PON ports

- Port isolation is on by default.

Enter VLAN configuration mode and enable port isolation.

```
AX3517(CONFIG/L2/VLAN)#usr-isolation enable
```

Enter VLAN configuration mode, turn off Port Isolation and turn on P2P. Among them, "disable standard" mode is applicable to normal P2P applications. `AX3517(CONFIG/L2/VLAN)#usr-isolation <<enable|disable-standard>`

Check the user isolation configuration.

```
AX3517(CONFIG/L2/VLAN)#show 101
```

4.2 Mac Address Table

AX3517/AX3515/AX3508/AX3502 maintains a MAC address table for packet forwarding. Each table item includes VLAN, MAC, port ID, type, virtual port ID and gem port ID. Layer 2 table items can be learned by AX3517/AX3515/AX3508/AX3502 switching chip hardware or created manually.

Layer 2 forwarding table entries can also be cleared through hardware based or software based aging.

The default time of the aging table is 300 seconds after the aging of the system. Manually created items remain in the table until manually deleted.

In the following cases, the MAC table entry shall be manually specified for the equipment. The designated user equipment with a specific MAC address is only allowed to access the specific AX3517/AX3515/AX3508/AX3502 port in the VLAN.

```
AX3517(CONFIG)#12 AX3517(CONFIG/L2)#bridge
```

```
AX3517(CONFIG/L2/BRIDGE)#fdb mac <MAC Address> {vid <VLAN ID>}
```

```
{interface <port-num>}
```

Displays the MAC address table.

```
AX3517(CONFIG/L2/BRIDGE)# brief-show mac-address AX3517(CONFIG/L2/BRIDGE)# show fdb
```

Delete the dynamic MAC address table.

```
AX3517(CONFIG/L2/BRIDGE)# flush fdb
```

4.3 Link Aggregation

The XGE port of AX3517/AX3515/AX3508/AX3502 operates as a layer 2 interface. Ports can be managed separately or as a link aggregation group (lag). A link aggregation group is a collection of multiple physical ports that operate as a single port. AX3517/AX3515/AX3508/AX3502 supports the configuration of static lag and LACP protocols.

4.3.1 Link Aggregation Interface Rate Control

When using port lag, please note:

- Ports at both ends must be configured as lag ports.
- A port can only belong to one lag. If the network administrator attempts to assign an XGE port that is already a member of lag B to lag a, the action will fail.
- All lag member ports of the same lag must have the same configuration, including bandwidth (1 Gbps), duplex

mode, and VLAN allocation.

- All ports in the lag group must be in the same spanning tree state.
- When a port belongs to a lag, its attributes (such as bandwidth, VLAN attribute, management status and duplex mode) cannot be configured separately.
- Before connecting the cable, activate the lag to avoid loop formation.
- Before deleting a lag, disconnect all lag port cables or close the lag port to avoid loop formation

4.3.2 Link Aggregation Group Load Balancing Rules

- SMAC (Source MAC)
- DMAC (Destination MAC)
- SMAC XOR DMAC (source MAC XOR destination DMAC)
- SIP (source IP address)
- DIP (destination IP address)
- SIP XOR DIP (source IP address XOR destination IP address)

The configuration commands are as follows:

```
AX3517(CONFIG/L2/PORT)#trunk <id> <name> xge | is <port>  
<srcMAC|dstMAC|srcdstMAC...> <static|lacp>
```

4.3.3 Link Aggregation Group Member Addition and Deletion

The device supports dynamic addition and deletion of link aggregation group members. The configuration commands are as follows:

- AX3502(PORT)#trunk-member 1 add interface "xge 4"
- AX3502(PORT)#trunk-member 1 delete interface "xge 1"

4.4 Link Aggregation

AX3517/AX3515/AX3508/AX3502 supports up to 4094 VLAN IDS (1-4094). Vid 1 and 4094 are reserved by the system for internal functions and are not allowed to be configured.

By default, AX3517/AX3515/AX3508/AX3502 ports are assigned to VLAN ID 1. These ports are untagged.

4.4.1 VLAN Management

When adding a port to a VLAN, the port can be configured as a tagged or untagged port. When configured as untagged, this VLAN ID is set as port PVID by default.

Layer 2 ports can belong to tagged ports of multiple VLANs and untagged ports of only one VLAN.

VLAN 1 is the default VLAN of each layer 2 port and cannot be deleted or modified

4.4.2 VLAN Configuration

4.4.2.1 Application Description

The service VLAN ID is 101. The uplink AX3517/AX3515/AX3508/AX3502 XGE port and the downlink AX3517/AX3515/AX3508/AX3502 OLT port are members of the system VLAN 101.

4.4.2.2 Instance Topology

This example takes the example of configuring AX3517/AX3515/AX3508/AX3502 basic data service.

- Create VLAN 101.

```
AX3517# configure
```

```
AX3517(CONFIG)# l2
```

```
AX3517(CONFIG/L2)# vlan
```

- AX3517(CONFIG/L2/VLAN)# vid 101 name 101 mode full-bridge
- Add xge1 as a member of VLAN 101.

```
AX3517(CONFIG/L2/VLAN)# interface xge 1 vid 101 untag
```

- Check the configuration information of VLAN 101.

```
AX3517(CONFIG/L2/VLAN)# show 101
```

4.4.3 VLAN Translation

The flow on the GPON system is identified by gem port. The gem port needs to be mapped to the corresponding VLAN on the switch. AX3517/AX3515/AX3508/AX3502 supports the configuration of VLAN translation table to complete the corresponding mapping.

- CLI enters VLAN command mode and configures VLAN translation.

```
AX3517(CONFIG/L2/VLAN)#translate slot <slot> port <port> ont <ONU- ID>
```

```
virtual-port <Vport-ID> svid <S-VID> cvid <C-VID> new-svid <New S- VID>
```

- Delete VLAN translation.

```
AX3517(CONFIG/L2/VLAN)# no translate slot <slot> port <port> ont
```

```
<ONU-ID> virtual-port <Vport-ID> svid <S-VID>
```

Key parameters are described in below table.

Field	Value Range	Default Values	Explain
Vport ID	Virtual Port ID: 1-8	N/A	Required, ONU ID / virtual port ID, specifies the virtual port of ONU.
C-VID	1-4095	N/A	Required, user VLAN ID. "4095" means untagged.
New S-VID	1-4094	N/A	Required, the new outer VLAN ID.
New C-VID	1-4095	4095	Optional, new inner VLAN ID, "4095" indicates no inner VLAN
CoS Action	copy Replace	copy	Optional, 802.1p priority processing mode.
CoS	0-7	7	Optional. It takes effect when cos action is replace, and 802.1p priority is set.

4.4.4 VLAN Stacking

Similar to vlan conversion, vlan stacking is that the switch adds a layer of 802.1Q vlan to the packet according to the GEM port and the inner and outer layer vlan

AX3517(CONFIG/L2/VLAN)#stacking slot <slot> port <port> ont <ONU- ID> virtual-port <Vport-ID> ovid <ovid><all|none|1-4095> ivid

<ivid><all|none|1-4095> stack-vid <stack-vid> new-cos <new-cos>

Field	Value Range	Default Values	Explain
Vport ID	Virtual Port ID: 1-12	N/A	Required, ONU ID/Virtual Port ID specifies the virtual port of the ONU.
OVID	ALL NONE 1-4095	N/A	Required, user VLAN ID. "all" means all VLans and "none" means Untagged.
I-VID	ALL NONE 1-4095	N/A	Required, user VLAN ID. "all" means all VLans and "none" means Untagged.
stack-vid	1-4095	N/A	Required, add new vlan
New-CoS	0-7	N/A	Optional, new priority. The default is to copy the outer priority of the original packet

4.5 Port Mirror

Configure another port to "mirror" the services on the port to be monitored. Connect the protocol analyzer to the mirror port to observe the services on the monitored port.

4.5.1 Port Mirroring Restrictions

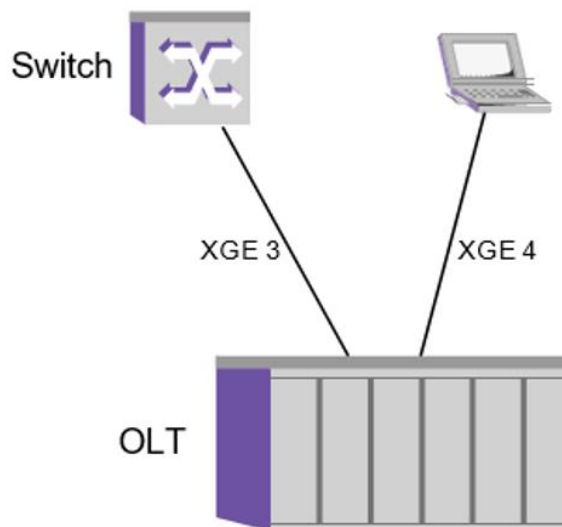
Configure another port to "mirror" the services on the port to be monitored. Connect the protocol analyzer to the mirror port to observe the services on the monitored port.

- The destination interface must be a single uplink interface rather than a group of interfaces. The destination interface cannot be the source interface.
- The system only supports one port image.
- Turn off the current port image when it is no longer needed.

4.5.1.1 Application Description

AX3517/AX3515/AX3508/AX3502 operates as a layer 2 switch, and its uplink port xge3 is abnormal. Xge4 will be configured as the image destination port to monitor xge3 port. Bidirectional data on xge3 is monitored.

4.5.1.2 Instance Topology



4.5.1.3 Configuration Requirements

The physical link of the port is normal.

4.5.1.4 Configure Task List

The task list of port mirroring configuration is as follows:

- Configure Port Mirroring

- Delete port mirror

Next, take the topology in Instance Topology figure as an example to introduce the detailed steps of each task.

4.5.1.5 Configure Port Mirroring

- Configure the mirror source port.
AX3517(CONFIG)#mirror-port receive xge 3
AX3517(CONFIG)#mirror-port transmit xge 3
- Configure the destination port of the image.
AX3517(CONFIG)#mirror-port mirror-port xge 4

4.5.1.6 Delete Port Mirroring Configuration

AX3517(CONFIG)#mirror-port mirror-port none

4.6 RSTP

AX3517/AX3515/AX3508/AX3502 system supports RSTP protocol.

4.6.1 RSTP Bridge Properties Ronfiguration

- Enable/Disable RSTP
AX3517(CONFIG/L2)#rstp <enable|disable>
- Enable/disable RSTP port management status
AX3517(CONFIG/L2)#rstp port-admin-state interface xge 1
<enable|disable>
- Bridge forwarding delay configuration
AX3517(CONFIG/L2/mstp)#forward <4-30>
- Handshake protocol time
AX3517(CONFIG/L2/rstp)#hellotime <1-10>
- Bridge maximum aging time
AX3517(CONFIG/L2/rstp)#maxage <6-40>

4.6.2 RSTP Priority Setting

- Bridge priority
AX3517(CONFIG/L2)#rstp priority <0..61440>
- Port priority
AX3517(CONFIG/L2)#rstp port-priority interface <xge|is|trunk>

<0..240>

4.6.3 Port Overhead Configuration

- Port overhead configuration

```
AX3517(CONFIG/L2)#rstp port-pathcost interface <xge|is|trunk>  
<1..200000000>
```

4.6.4 Viewing the RSTP Configuration

- View the global RSTP configuration

```
AX3517(CONFIG/L2)#rstp show
```

- View port RSTP configuration

```
AX3517(CONFIG/L2)#rstp show port interface <xge|is|trunk>
```

4.7 MSTP

AX3517/AX3515/AX3508/AX3502 The system supports MSTP protocol.

4.7.1 MSTP Bridge Property Configuration

- Turn MSTP On / Off

```
AX3517(CONFIG/L2)#mstp <enable|disable>
```

- Bridge Forwarding Delay Configuration

```
AX3517(CONFIG/L2/mstp)#forward-time <4-30>
```

- Handshake Protocol Time

```
AX3517(CONFIG/L2/mstp)#hello-time <1-10>
```

- Maximum Aging Time Of Bridge

```
AX3517(CONFIG/L2/mstp)#max-age <6-40>
```

- Maximum Hops

```
AX3517(CONFIG/L2/mstp)#max-hops <1-40>
```

4.7.2 MSTP Configuration

- Configuration Instance

```
AX3517(CONFIG/L2)#mstp configuration instance <1-15> vlan <vlan range ex>
```

- Mst Name

```
AX3517(CONFIG/L2)#mstp configuration name <Configuration name>
```

- Delete Mst Name

```
AX3517(CONFIG/L2)#mstp configuration no name
```

- Mst Level
AX3517(CONFIG/L2)#mstp configuration revision<0-65535>
- Delete Mst Level
AX3517(CONFIG/L2)#mstp configuration no revision

4.7.3 MSTP Priority Configuration

- Bridge Priority
AX3517(CONFIG/L2)#mstp instance <0-15> priority <bridge priority in increments of 4096>
- Port Priority
AX3517(CONFIG/L2)# mstp instance <0-15> port-priority interface xge <port> <priority>
- Port Cost
AX3517(CONFIG/L2)# mstp instance <0-15> port-pathcost interface xge <port> <priority>

4.7.4 View MSTP Status

- View MSTP Configuration
AX3517(CONFIG/L2)# mstp show configuration
- View MSTP Port Status
AX3517(CONFIG/L2)# mstp show instance <0-15> port interface xge
<port>
- View MSTP Status
AX3517(CONFIG/L2)# mstp show instance <0-15>

4.8 Relay Options

DHCP and PPPoE support relay options. Add option information to the request message received from DHCP / PPPoE client to DHCP / PPPoE server to identify the user's location information.

- Turn on the relay option.
AX3517(CONFIG/L2/VLAN)# dhcp-option 0 enable AX3517(CONFIG/L2/VLAN)# pppoe-option 0 enable
- Turn off the relay option.
AX3517(CONFIG/L2/VLAN)# dhcp-option 0 disable AX3517(CONFIG/L2/VLAN)# pppoe-option 0 disable
- Check the relay option configuration.
AX3517(CONFIG/L2/VLAN)# show vlan-option

4.9 Loop Detection

AX3517/AX3515/AX3508/AX3502 supports the loop detection function. OLT sends detection messages regularly. When a loop is generated, it will detect and report to the police.

AX3517(CONFIG/L2)# loop-detect <enable|disable>

AX3517(CONFIG/L2)# loop-detect direction < uplink|downlink> AX3517(CONFIG/L2)# loop-detect show

See below table for the description of key parameters

Field	Value Range	Default Values	Explain
Direction	Uplink downlink both	Both	Optional, loop detection direction.
Ether-type	0x600-0xffff	0x9900	Optional, second index, from index.
Interval	10-86400	60	Optional, the time interval of sending detection message, in seconds.
Recover-time	1-1440	1440	Optional, failure recovery time, in minutes.

5 L3 Configuration

This section describes the configuration of three-layer SVI on AX3517/AX3515/AX3508/AX3502.

5.1 SVI Concept

When data packets communicate in layer 2, they can only be forwarded in the same VLAN. In order to enable data packets to be transmitted between different VLANs, three-layer communication is required.

AX3517/AX3515/AX3508/AX3502 uses SVI (switch virtual interface) to enable AX3517/AX3515/AX3508/AX3502 to route data packets between VLANs.

By configuring the switching virtual interface (SVI), one or more AX3517/AX3515/AX3508/AX3502 XGE ports can be configured as a virtual single interface, and the virtual interface is assigned an IP address to activate routing.

Only one SVI can be configured for each VLAN.

SVI is a three-layer interface, and the packet processing on the three-layer interface includes two-layer switching and three-layer routing. Layer 3 routing forwards packets according to the routing table.



In the topology, AX3517/AX3515/AX3508/AX3502 is connected to the network through a three- layer switch. The uplink layer-3 switch works in layer-3 mode. SVI 500 (10.0.0.2 / 24) has been configured, and SVI 500 (10.0.0.1 / 24) has been configured for AX3517/AX3515/AX3508/AX3502.

The next section describes the configuration steps of SVI.

This configuration example uses the network topology shown in above figure. Configure SVI for xge4 port of AX3517/AX3515/AX3508/AX3502 to establish three-layer communication between AX3517/AX3515/AX3508/AX3502 and switch.

5.2 Create SVI

- To configure SVI, you need to select route mode when creating VLAN.
- Create and manage VLANs according to network planning. In this example, VLAN 500 is configured as route mode.

```
AX3517(CONFIG/L2/VLAN)# vid 500 name 500 mode routed
```

- Add port xge4 as a tagged member of VLAN 500.

```
AX3517(CONFIG/L2/VLAN)# interface xge 4 vid 500 tag
```

- Configure the IP address of SVI (this example uses 10.0.0.1/24).

```
AX3517(CONFIG/L2/VLAN)# exit
```

```
AX3517(CONFIG/L2)# exit
```

```
AX3517(CONFIG)# l3
```

```
AX3517(CONFIG/L3)# interface
```

```
AX3517(CONFIG/L3/INTERFACE)# interface vlan 500:1 ip 10.0.0.1
```

```
netmask 255.255.255.0
```

- Check whether the SVI configuration is successful.

```
AX3517(CONFIG/L3/INTERFACE)# show interface
```

5.3 Configure ARP

Address resolution protocol (ARP) is used to map IP address to MAC address. Refer to RFC 826 for details.

The fields of ARP table are IP address, MAC address and interface number, etc. ARP entries can be either dynamic or static. Dynamic items are automatically learned by the system, and static items are manually specified.

Create dynamic ARP table entries when:

AX3517/AX3515/AX3508/AX3502 communicates with uplink and downlink network equipment above layer 3.

- Configure static ARP table entries.

```
AX3517(CONFIG)# l3 AX3517(CONFIG/L3)# arp
```

```
AX3517(CONFIG/L3/ARP)# interface xge 4 ip 10.0.0.2 mac
```

```
00:00:00:88:88:88 vid 500
```

- View ARP table entries.

```
AX3517(CONFIG/L3/ARP)# show arp
```

- Clear the ARP table entry.

```
AX3517(CONFIG/L3/ARP)# flush arp <vid> <2..4094>
```

5.4 Configure IP Route

When working as a layer 3 switch, AX3517/AX3515/AX3508/AX3502 maintains the routing table for packet forwarding. Including destination IP address, subnet mask, gateway address and metric. It can be created dynamically or configured manually.

- Configure static routing.

```
AX3517#ip route <network> netmask <mask> gateway <ipaddr>
```

6 GPON Configuration

AX3517/AX3515/AX3508/AX3502 complies with ITU-T g.984/g.988 series standards.

This chapter describes the configuration steps of all passive optical networks (gpons):

- Configure ONU authentication
- Configure ONU registration
- Configure ONU service flow
- OLT management
- ONU management
- Configure FEC
- Configure downlink encryption
- PON optical power measurement

6.1 Configure ONU Authentication

After accessing OLT, ONU needs to go through the initial authentication process. ONU without authentication cannot generate normal data link. AX3517/AX3515/AX3508/AX3502 supports five authentication modes:

- Sn certification
- Password authentication
- Sn & password authentication
- Disable authentication
- Loid certification
- Loid & password authentication

The system defaults to Sn (serial number) authentication, and the serial number of ONU can be viewed at the bottom of ONU.

Password uses the registration ID in the xgpon / xgspon system.

Each AX3517/AX3515/AX3508/AX3502 GPON downlink port (hereinafter referred to as PON port) can be connected with a certain number of onus (the specific number is determined by the port mode. For example, the maximum number of gpons of combo board can be connected is 128). Since these ONUs are connected to

the same physical PON port, it is recommended to enable authentication and bind different ONU IDs for onus for management convenience.

Use the following command to configure the ONU authentication mode:

```
AX3517(slot-1)# gpon ont-authentication  
<snonly|password|snandpassword|disabled|loidonly|loidandcheckcode>
```



Caution: If the authentication mode is modified, the system will automatically clear all ONU related configurations.

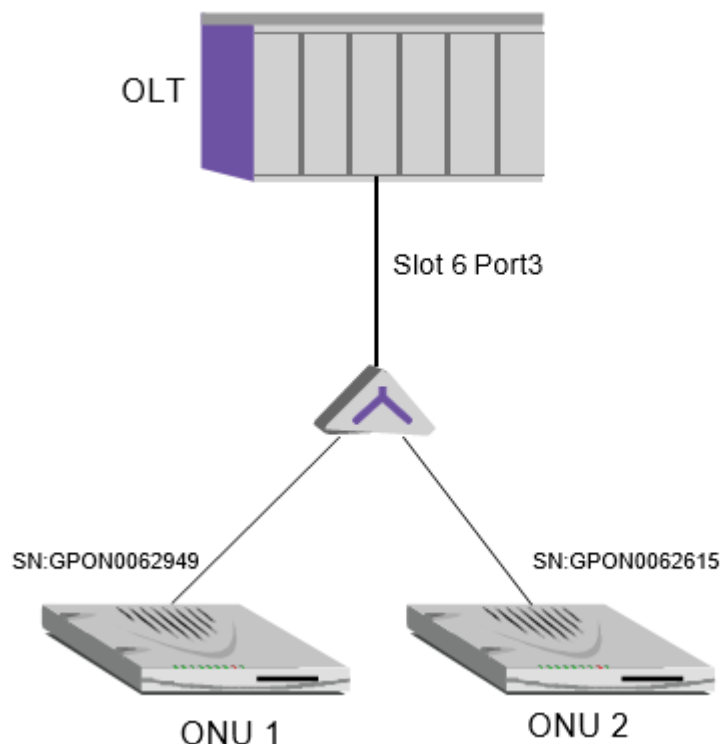
6.2 Configure ONU Registration

When the OLT turns on Sn authentication, the binding ONU Sn and ONU Id need to be configured.

6.2.1 Application Description

In this example, ONU1 and ONU2 need to be successfully registered on the AX3517/AX3515/AX3508/AX3502 system.

6.2.2 Instance Topology



As shown in above figure, the downlink olt1 / 1 port of AX3517/AX3515/AX3508/AX3502 is connected with onu1 and onu2 through optical splitter.

6.2.3 Configure Task List

The tasks of configuring ONU registration are as follows:

- Configure ONU Sn and ONU ID binding
- View ONU registration status

6.2.4 Configure the ONU SN and ONU ID Binding

There are 64 logical ports in each OLT downlink port. Onus connected to the same OLT downlink port can be bound to any ONU ID. In this example, ONU ID of onu1 is 1 and ONU ID of onu2 is 2.

- Enter the configure terminal command mode.

```
AX3517# slot 6
```

```
AX3517(slot-1)#
```

- Enter the OLT port configuration command mode.

```
AX3517(slot-1)# interface gpon-olt 1/1
```

```
AX3517(slot-1 /if-gpon-olt-1/1)#
```

- Enter the ONU configuration command mode to configure the binding of ONU ID and sn.

```
AX3517(slot-1/if-gpon-olt-1/1)# ont 1
```

```
AX3517(slot-1/if-gpon-olt-1/1)# sn GPON6cefc60c AX3517(slot-1/if-gpon-olt-1/1)# exit
```

```
AX3517(slot-1/if-gpon-olt-1/1)# ont 2
```

```
AX3517(config-if-gpon-ont-1/1/2)# sn GPONc6543466
```



Note: The SN of ONU can be found on the bottom cover of ONU.

6.2.5 View Registration Status of ONU

```
AX3517(slot-1)# brief-show slot 6 ont-info
```

```
Total Ont Number :      2
```

```
Active Ont Number:      2
```

ONT	SN	Status	ind	Auth	Reason
1/1/1	GPON6CEFC60C	ready	auto	snonly	none
1/1/2	GPONC6543466	ready	auto	snonly	none

Result description: when the status is "ready", it indicates that the ONU has successfully completed registration.

6.2.6 Delete ONU

Delete ONU

```
AX3517(slot-1)# interface gpon-olt 1/1
```

```
AX3517(slot-1/if-gpon-olt-1/1)# no ont 1
```

```
AX3517(slot-1/if-gpon-olt-1/1)# no ont 2
```

6.3 Configure ONU Service

GPON is based on stream management and forwarding.

6.3.1 Concept Introduction

- Virtual Port

AX3517/AX3515/AX3508/AX3502 uses virtual port to define specific flows. The flow profile describes the characteristics of each flow. Each flow is mapped to a virtual port. According to the application model, one or more virtual ports can be bound to the same t-cont.

- T-CONT

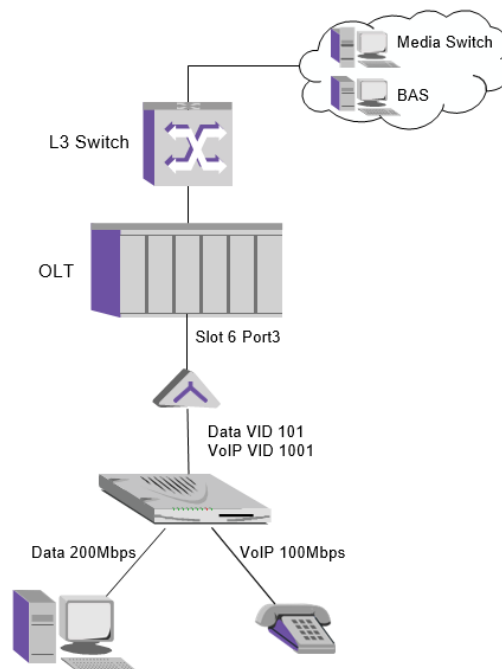
G. 984.3 t-cont is used to describe the uplink bandwidth, and three bandwidth parameters are defined: fixed bandwidth, guaranteed bandwidth and maximum bandwidth. According to the different needs of users, five types of t-cont are established: type1-type5. As shown in below table.

Traffic descriptor component	Type 1	Type 2	Type 3	Type 4	Type 5
Fixed BW	R_F				R_F
Assured BW		R_A	R_A		R_A
Maximum BW	$R_M = R_F$	$R_M = R_A$	$R_M > R_A$	R_M	$R_M \geq R_F + R_A$
Additional BW eligibility	None	None	NA	BE	Any

6.3.2 Application Description

In this example, data and voice services are configured for users. The maximum uplink bandwidth of data services is 200Mbps, and the uplink bandwidth of voice services is guaranteed to be 256Kbps.

6.3.3 Topology Instance



AX3517/AX3515/AX3508/AX3502 is connected to the network through uplink port xge1, and PC and telephone are connected to ONU 1 / 1 / 1.

Configuration requirements:

- ONU has completed registration.
- The ONU WAN interface configuration is completed (usually according to the factory default configuration required by the operator), data service VLAN ID 101 and voice service VLAN ID 1001. See the ONU configuration manual for specific configuration.
- The uplink switch has been configured according to the network planning.

6.3.4 The Task List of Configuration

Configure ONU business tasks as follows:

- Configure uplink port and VLAN
- Configure business profile
- Apply GPON profile to ONU
- Voice service configuration
- Configure VLAN translation
- Delete the ONU service configuration of this instance

6.3.5 Configure the Uplink Port and the VLAN

- Configure the XGE1 port enable. Please refer to Port Attribute.
- Create VLAN 101 and VLAN 1001, and configure XGE 1 and IS 1 / 1 as VLAN Tagged members.

Please refer to VLAN Configuration.

6.3.6 Configure Flow Service Profile

The flow profile is used to describe the upstream attributes. Enter the line card command mode, configure the flow profile,

```
AX3517(slot-1)# gpon profile flow id <ID1> <ID2> name <flow name>
```

```
{uni-type <ethernet-uni|ip-host|veip>} {uni_bitmap <bitmap>} {upmap- type  
<vlanId|priorityBits|vlanIdAndPriorityBits>} {vlanId <VLAN ID Start> <VLAN ID Stop>} {pri-bitmap  
<bitmap>} {vport <ID>}
```

See below table for the description of key parameters.

Field	Value Range	Default Values	Explain
ID1	1-128	N/A	Required: the first index and the primary index. When multiple virtual ports need to be bound to the same TCONT, selecting the primary index means that a series of virtual ports with the same primary index are selected.
ID2	1-127	N/A	Required, secondary index, secondary index.
uni-type	ethernet-uni ip-host veip	N/A	Required. The user port mode is determined by the ONU. Select the appropriate type according to different types of onus. Select VEIP for HGU and Ethernet uni for SFU.
uni_bitmap	0x00-0xff	N/A	Required, user port mask, specifies the selected port ID, for example, 0x01 is port 1, 0x03 is port 1 ~ 2.
upmap-type	vlanId priorityBits vlanIdAndPriorityBits	N/A	Required, upstream mapping type.
vlanId	0-4095	N/A	Compulsory. The VLAN ID range filtered by the upstream VLAN supports up to 12 VLANs.
pri-bitmap	0x0-0xff	N/A	Required, priority mask, which specifies the selected priority. For example, 0x01 is 0, 0x03 is 0, 1.
vport	1-8	N/A	Required to specify the defined virtual port ID.

In this example, the ONU uplink has two service flows: data and voice, and the VLAN IDs are 101 and 1001 respectively.

```
AX3517# slot 6
```

```
AX3517(slot-1)# gpon profile flow id 2 1 name flow_1 uni-type veip uni-bitmap 0x1 upmap-type vlanId  
101 101 pri-bitmap 0xff vport 1
```

```
AX3517(slot-1)# gpon profile flow id 2 2 name flow_1 uni-type veip uni-bitmap 0x1 upmap-type vlanid
1001 1001 pri-bitmap 0xff vport 2
```

View the GPON profile.

```
AX3517(slot-1)# brief-show configuration running
```

Note: flow ID 1 is recommended as the default configuration without modification.

6.3.7 Configure the Rate Control Profile

The rate control profile is used to describe rate control.

Enter the configure terminal command mode and configure the rate control profile,

```
AX3517(slot-1)# gpon profile rate-ctrl id <ID> name <Name> sir
```

```
<Rate> pir <Rate>
```

The key parameters are described in below figure.

Field	Value Range	Default Values	Explain
ID	1-128	N/A	Required, profile index.
sir	128-1244160	N/A	Required, guaranteed bandwidth, unit Kbps, configuration granularity 64Kbps.
pir	128-1244160	N/A	Required, peak bandwidth, unit: Kbps, configuration granularity: 64Kbps.

In this example, there is no rate restriction requirement. The two streams are set with a bidirectional rate of 1000Mbps, and can share the same profile.

```
AX3517(slot-1)# gpon profile rate-ctrl id 1 name rate_1 sir 1024000 pir 1024000
```

6.3.8 Configure Virtual Port Service Profile

The virtual port service profile is used to define the queue attributes and rate of the flow. The rate parameters are described by the rate control profile, that is, they need to be bound with the rate control profile.

Enter the configure terminal command mode and configure the virtual port service profile.

```
AX3517(slot-1)# gpon profile vportsvc id <Index> name <Name> us- pri <Priority> usratectrl-id <Rate
Control Profile ID>dsratectrl-id
```

```
<Rate Control Profile ID>
```

The key parameters are described in below table.

Field	Value Range	Default Values	Explain
Index	1-128	N/A	Required, profile index.
us-pri	0-7	N/A	Required, the priority of the uplink queue.
Usratectrl -id	0-128	N/A	Required, pointing to the rate control profile index, "0" indicates no speed limit.
Dsratectrl -id	0-128	N/A	ditto.

In this example, there is no rate limit requirement. Set the bidirectional rate of 1000Mbps and bind the corresponding rate control profile. Voice data stream has a higher priority of 2.

```
AX3517(slot-1)# gpon profile vportsvc id 1 name vportsvc_1 us-pri
```

```
0 usratectrl-id 1 dsratectrl-id 1
```

```
AX3517(slot-1)# gpon profile vportsvc id 2 name vportsvc_1 us-pri
```

```
2 usratectrl-id 1 dsratectrl-id 1
```

6.3.9 Configure DBA Profile

DBA profile is used to describe DBA (uplink dynamic bandwidth allocation) attributes, including t-cont type and bandwidth parameter value.

Enter the configure terminal command mode and configure the DBA profile,

```
AX3517(slot-1)# gpon profile dba id <ID> name <Name>
```

```
<type1|type2|type3|type4|type5> [fix <Bandwidth>] [assure <bandwidth>] [max <bandwidth>]
```

The key parameters are described in below table.

Field	Value Range	Default Values	Explain
ID	1-128	N/A	Required, profile index.
type	Type1, Type2, Type3, Type4, Type5	N/A	Required, t-cont type.
fix	256-1151168	N/A	Optional, fixed bandwidth, unit Kbps, configuration granularity 64Kbps.
assure	256-1151040	N/A	Optional, fixed bandwidth, unit Kbps, configuration granularity 64Kbps.
max	256-1244160	N/A	Optional, fixed bandwidth, unit Kbps, configuration granularity 64Kbps.

In this example, the maximum bandwidth of 200Mbps is configured for data service and 256K guaranteed bandwidth is configured for voice service.

```
AX3517(slot-1)# gpon profile dba id 2 name dba_2 type3 assure 256 max 204800
```

6.3.10 Configure T-Cont Service Profile

The t-cont service profile is used to describe the t-cont attribute and is bound to the DBA profile.

Enter the configure terminal command mode and configure the t-cont service profile,

```
AX3517(slot-1)# gpon profile tcont-svc id <ID> name <Name> dba-id
```

<ID>

The key parameters are described in below table.

Field	Value Range	Default Values	Explain
ID	1-128	N/A	Required, profile index.
dba-id	1-128	N/A	Required, DBA profile index.

In this example, the maximum bandwidth of 200Mbps is configured for data service and 256K guaranteed bandwidth is configured for voice service. Bind corresponding profiles respectively.

```
AX3517(slot-1)# gpon profile tcont-svc id 2 name tcontsvc_2 dba-id 2
```

6.3.11 Configure T-Cont Binding Profile

The t-cont binding profile is used to bind virtual ports and t-cont.

Enter the configure terminal command mode to configure the t-cont binding profile,

```
AX3517(slot-1)# gpon profile tcont-bind id <ID> v-port <Virtual Port ID> name <Name> {vportsvc-id <ID>}  
{tcont-id <ID>}{tcontsvc-id <ID>}
```

The key parameters are described in below table.

Field	Value Range	Default Values	Explain
ID	1-128	N/A	Required, profile index Required. The index of the virtual port corresponds to the vport ID in the flow profile.
v-port	1-8	N/A	
vportsvc-id	1-128	N/A	Required, virtual port service profile index.
tcont-id	1-8	N/A	Required, t-cont ID, specified by the user.
tcontsvc-id	1-128	N/A	Required, t-cont service profile index.

In this example, virtual ports 1 and 2 carry data and voice services respectively, and have different requirements for upstream bandwidth. The T-CONT of the type3 (assured-maximum) DBA is bound. The maximum bandwidth of virtual port 1 is 200M, and that of virtual port 2 is more High priority guarantees 256k of bandwidth.

```
AX3517(slot-1)# gpon profile tcont-bind id 2 v-port 1 name tcontbind_2 vportsvc-id 1 tcont-id 1 tcontsvc-id 2
```

```
AX3517(slot-1)# gpon profile tcont-bind id 2 v-port 2 name tcontbind_2 vportsvc-id 2 tcont-id 1 tcontsvc-id 2
```

View the GPON profile

```
AX3517(slot-1)# show configuration running gpon-profile
```

6.3.12 GPON Profile Application

After the GPON profile is configured, it can be used by all ONUs. The configured profile needs to be delivered to the ONU. The ONU receives the profile information and takes effect after completing the local settings.



Caution: When the GPON profile is used by the ONU, modification and deletion are not allowed.

CLI enters the ONU command mode, creates a virtual port on the ONU and delivers the profile configuration.



Note: The virtual port index must be the same as the vport ID in the Flow profile.

```
AX3517(slot-1)# interface gpon-olt 1/1 AX3517(slot-1/if-gpon-olt-1/1)# ont 1
```

```
AX3517(slot-1/if-gpon-olt-1/1/1)# virtual-port <ID> {port
```

```
<lock|unlock>}
```

```
AX3517(slot-1/if-gpon-olt-1/1/1)# service flow-profile <ID> tcont- bind-profile <ID>
```

Key parameters explainain are as follows in below table.

Field	Value range	Default values	Explain
Virtual-port	1-8	N/A	Required, profile index.
flow-profile	1-128	N/A	Required, specifies a Flow profile.
tcont-bind-profile	1-128	N/A	Required, specifies the T-CONT binding profile.

In this example, two virtual ports 1 and 2 need to be created to carry data services and voice services respectively.

```
AX3517(slot-1)# interface gpon-olt 1/1
```

```
AX3517(slot-1/if-gpon-olt-1/1)# ont 1
```

```
AX3517(slot-1/if-gpon-olt-1/1/1)# virtual-port 1 port unlock AX3517(slot-1/if-gpon-olt-1/1/1)# virtual-port 2 port unlock Apply the GPON profile to the ONU.
```

```
AX3517(slot-1/if-gpon-olt-1/1/1)# service flow-profile 2 tcont-  
bind-profile 2
```

Check the ONU configuration.

AX3517(slot-1)# brief-show configuration running

6.3.13 Voice Service Configuration

Below table provides basic information about configuring voice from the OLT.

- Create a voice profile.

```
AX3517(slot-1)# gpon profile voip-sip-agent id <ID> name
<name> proxy-server <ip-addr> registrar-server <ip-addr> tcp-port
<port-id>
```

Field	Value range	Default values	Explain
Proxy-addr	0.0.0.0~255.255.255.255	N/A	Required, the IP address of the SIP proxy server.
External-proxy-addr	0.0.0.0~255.255.255.255	N/A	Required, the IP address of the SIP outbound proxy server.
Registering-addr	0.0.0.0~255.255.255.255	N/A	Required, the IP address of the SIP registrar server.
Tcp-port	0~65535	5060	Optional, the SIP protocol port number.

In this example, the configuration is as follows.

```
AX3517(slot-1)# gpon profile voip-sip-agent id 1 name 1 proxy- server 192.168.2.97 registrar-server
192.168.2.97 tcp-port 5060
```

- Applying Voice profiles to ONU.

```
AX3517(slot-1/if-gpon-olt-1/1/1)#voip-service sip <port-list> agent-id <profile index> media-id <profile
index> phone-num <WORD> username <WORD> password <WORD> user-id <profile index>
```

Key parameters explain the following table.

Field	Value Range	Default Values	Explain
Pots-uni	1~2	N/A	Required, POTS port number.
Agent-id		N/A	Required, set the sip proxy configuration file index
Media-id		N/A	Required, set the voip media profile index
Phone-number		N/A	Required, phone number.
Username		N/A	Required, registered user name..
Password		N/A	Required, registration password.
User-id		N/A	Required, set the sip user profile index

In this example, the configuration is as follows.

```
AX3517(slot-1)# voip-service sip 1-2 agent-id 1 media-id 1 phone-
```

num 123123 username 1 password 123 user-id 1

6.3.14 Configure VLAN Translation

The flow on the GPON system is identified by GEM Port. The switch needs to map the GEM Port to the corresponding VLAN. The AX3517/AX3515/AX3508/AX3502 supports configuring the VLAN translation table to complete the corresponding mapping.

- The CLI enters the OLT command mode to configure VLAN translation.

```
AX3517# configure AX3517(CONFIG)# l2 AX3517(CONFIG/L2)# vlan
```

```
AX3517(CONFIG/L2/VLAN)# translate slot <slotId> port <portId> ont <ontId> virtual-port
<vportId> cvid <C-VID> new-svid <New S-VID> new-cvid <New C-VID> cos <copy|replace> new-cos
<cos>
```

- Remove VLAN translation.

```
AX3517(CONFIG/L2/VLAN)# no translate slot <slotId> {port
<portId> ont <ontId> virtual-port <vportId> cvid <C-VID>} AX3517#(CONFIG/L2/VLAN)# brief-
show vlan-translate
```

The key parameters are described in below table.

Field	Value Range	Default Values	Explain
Slot	1-10	N/A	Required, the slot number of the line card.
Port	1-16	N/A	Required, PON port number.
Ont	1-256	N/A	Required, ONU ID number.
Virtual-port	1-8	N/A	Required, the virtual port number.
C-vid	1-4095	N/A	Required. User VLAN ID. "4095" means Untagged.
New-svid	1-4094	N/A	Required, the new outer VLAN ID.
New-cvid	1-4095	4095	Optional, new inner VLAN ID, "4095" means no inner VLAN
CoS Action	copy Replace	copy	Optional, 802.1p priority processing method. Optional. It takes effect when the CoS Action is replace and sets the 802.1p priority.
New-cos	0-7	7	

In this example, the data VLAN 101 and the voice VLAN 1001 upstream do not change, the configuration is as follows.

```
AX3517(CONFIG/L2/VLAN)# translate slot 1 port 1 ont 1 virtual-port
```

```
1 svid 101 new-svid 101
```

```
AX3517(CONFIG/L2/VLAN)# translate slot 1 port 1 ont 1 virtual-port
```

```
2 svid 1001 new-svid 1001
```

Check the ONU configuration.

AX3517(slot-1)# brief-show configuration running<Slot id>

6.3.15 Deleting ONU Service Configuration



Caution: Due to the association of ONU configurations, it is recommended to follow a specific order when deleting configurations, otherwise it may become invalid.

- Remove VLAN translation.

```
AX3517(CONFIG/L2/VLAN)# no translate slot 1 port 1 ont 1
```

```
virtual-port 1 svid 101
```

```
AX3517(CONFIG/L2/VLAN)# no translate slot 1 port 1 ont 1
```

```
virtual-port 2 svid 1001
```

- Delete ONU services.

```
AX3517(slot-1)# interface gpon-olt 1/1 AX3517(slot-1/if-gpon-olt-1/1)# ont 1 AX3517(slot-1/if-  
gpon-olt-1/1/1)# no service
```

```
AX3517(slot-1/if-gpon-olt-1/1/1)# no virtual-port 1 AX3517(slot-1/if-gpon-olt-1/1/1)# no virtual-port 2
```

- Delete the GPON profile.



Note: GPON profile "1" is the system default profile and cannot be deleted. The following commands are examples only.

```
AX3517(slot-1)# no gpon profile <profile Name> <profile ID>.
```

6.4 OLT Management

6.4.1 OLT Port Management Status

The PON port can be turned on or off by setting the management status of the port. By default, the PON port management state is enabled.

Use the CLI command shutdown to change the management state of the port to closed, and use the CLI command no shutdown to change the management state of the port to open.

```
AX3517(slot-1/if-gpon-olt-1/1)# shutdown AX3517(slot-1/if-gpon-olt-1/1)# no shutdown
```

6.4.2 Optical Transceiver Diagnosis

PON port optical module parameters can be obtained through CLI commands. Including bias current, supply voltage, module temperature, transmit optical power, receive optical power and other information.

```
AX3517(slot-1)#brief-show slot 6 interface gpon-olt 1/1 optical- info ont 1 received-power
```

6.5 ONU Management

The ONU is usually located on the user side. To facilitate management, AX3517/AX3515/AX3508/AX3502 provides CLI commands to manage ONUs.

6.5.1 View ONU Basic Information

AX3517/AX3515/AX3508/AX3502 provides CLI commands to obtain basic online ONU information.

- View ONU capability status information.

```
AX3517(slot-1)# brief-show slot 6 interface gpon-olt 1/1 ont 1 brief
```

- View ONU version information.

```
AX3517(slot-1/if-gpon-olt-1/1)# brief-show slot 6 interface gpon- olt 1/1 ont 1 summary
```

- View ONU optical module information.

```
AX3517(slot-1/if-gpon-olt-1/1/1)# brief-show slot 6 interface gpon-olt 1/1 ont 1 optical-info
```

- View the received optical power of the OLT for a specific ONU.

```
AX3517(slot-1/if-gpon-olt-1/1/1)#brief-show slot 6 interface gpon- olt 1/1 optical-info ont 1 received-  
power
```

- View the optical power information of all ONUs of the OLT.

```
AX3517(Slot-1/if-gpon-olt-1/1/1)#brief-show all ont-transceiver
```

ONT	Voltage(V)	Rx power(dBm)	Tx power(dBm)	Bias current(mA)
Temperature(Centigrade)				
10/12/2	3.34	-13.8000	5.8900	33.628
48.29				
10/12/3	0.00	0.0000	0.0000	0.000
0.00				
10/12/4	0.00	0.0000	0.0000	0.000
0.00				

6.5.2 Activate/Deactivate ONU

The deactive state indicates that the ONU is prohibited from being used. The ONU can be activated using the active command.

The default state of an ONU is active.

```
AX3517(slot-1)# interface gpon-olt 1/1
```

```
AX3517(slot-1/if-gpon-olt-1/1)# ont 1
```

```
AX3517(slot-1/if-gpon-olt-1/1/1)# deactive|active
```

6.5.3 Turn ON/OFF ONU

The user can use the disable command to turn off the ONU illuminator. The ONU illuminator can be turned on using the enable command.

```
AX3517(slot-1)# interface gpon-olt 1/1
```

```
AX3517(slot-1/if-gpon-olt-1/1)# ont 1
```

```
AX3517(slot-1/if-gpon-olt-1/1/1)# <disable|enable>
```

When the unregistered ONU does not emit light (the ONU is in the O7 state), you can use the CLI command to turn on the light of all ONUs under the PON port.

```
AX3517(slot-1/if-gpon-olt-1/1)# all-ont enable
```

6.5.4 ONU Reset

AX3517/AX3515/AX3508/AX3502 provides CLI commands to reset a specific ONU.

For example, to restart ONU 1/1/1, enter the following CLI command:

```
AX3517(slot-1/if-gpon-olt-1/1/1)# reset
```

6.5.5 ONU Port Management

AX3517/AX3515/AX3508/AX3502 provides CLI commands to configure ONU ETH UNI port parameters

The user can use the Deactivate command to enable the ONU ETH_UNI port. The ONU ETH_UNI port can be enabled by using the Activate command, and the default port is enabled.

```
AX3517(slot-1/if-gpon-olt-1/1/1)# <activate|deactivate>
```

```
AX3517(slot-1/if-gpon-olt-1/1/1)# eth-uni <unild> config
```

```
AX3517(slot-1)# brief-show slot 6 interface gpon-olt 1/1 ont 1 eth-uni 1
```

The key parameters explain are listed in below figure.

Field	Value Range	Default Values	Explain
ID	1-24	N/A	Required, UNI port number.
I2I3	L2 L3 Either	N/A	Optional, Port Mode: Bridged/Routed
Mtu	64~8192	N/A	Optional, maximum frame length.
Pause-time	0~65535	N/A	Optional, port flow control. "0" means to turn off the flow control function.
type	0~254	N/A	Optional, port type. See G.988 Table 9.1.5-1 for details
pppoe-filter	Enable Disable	N/A	Optional, PPPoE packet filtering.

Field	Value Range	Default Values	Explain
wiring	DCE DTE Auto	N/A	Optional, Ethernet port type.
loop	No-loop Loop3	N/A	Optional, port loopback.
Arc	Enable Disable	N/A	Optional, alarm suppression.
Arc-interval	0~255	N/A	Optional, alarm suppression interval.
Speed	10m 100m 1000m 10g 20g 5g 25g 40g Auto	N/A	Optional, the interface rate.
Duplex	Full Half Auto	N/A	Optional, interface duplex mode.

6.5.6 PoE Port Management

PoE (Power over Ethernet, Power over Ethernet, also known as remote power supply) means that the device uses the twisted pair cable to remotely supply power to the PD (Powered Device, Powered Device) attached to the remote network through the Ethernet electrical port to achieve power supply. A mechanism in parallel with data transfer.

The PoE system consists of three parts: PSE, PD, and PI:

- PSE (Power-Sourcing Equipment, power supply equipment): It consists of power supply and PSE functional modules. It can realize PD detection, PD power information acquisition, remote power supply, power supply monitoring, and equipment power-off functions.
- PD: A device that receives power from the PSE. There are standard PDs and non-standard PDs. Standard PDs refer to PD devices that comply with the 802.3af standard. Common PDs include IP phones, wireless APs, and network cameras.
- PI (Power Interface): The interface between the PSE/PD and the network cable, that is, the RJ-45 interface.

The user can use the command to enable the PoE function of the port.

```
AX3517(slot-1/if-gpon-olt-1/1/1)# eth-uni <unild> poe
```

```
<enable|disable>
```

Configure the PoE parameters of the port:

```
AX3517(slot-1/if-gpon-olt-1/1/1)# eth-uni <unild> poe
```

```
AX3517(slot-1)#brief-show slot 6 interface gpon-olt 1/1 ont 1 eth- uni 1
```

Key parameters explain are listed in below table.

Field	Value Range	Default Values	Explain
Mode	Signal Spare	N/A	Optional, Ethernet port PoE power supply mode. Signal line mode or idle line mode.
Priority	Critical High Low	N/A	Optional, port power supply priority
Max-power-class	Default Class0 Class1 Class2 Class3 Class4	N/A	Optional, PSE power class.

6.5.7 PoE Port Management

Users can configure the port rate limit based on ETH_UNI using the command:

```
AX3517(slot-1/if-gpon-olt-1/1/1)# rate-limit eth-uni <unild>
<upstream|downstream> <cir> <pir>
```

6.5.8 Mac Address

The user can use the command to configure the ONU MAC-Limit, which supports two configuration methods, and select the corresponding configuration according to the specific implementation of the ONU:

Based on MAC Bridge Service:

```
AX3517(slot-1/if-gpon-olt-1/1/1)# mac-limit <value>
```

Based on MAC Bridge Port:

```
AX3517(slot-1/if-gpon-olt-1/1/1)# mac-limit eth-uni <unild>
<value>
```

6.5.9 Mac-Filter

MAC address filtering means that the access device checks the source MAC address or destination MAC address carried in user packets, and filters the packets carrying the specified MAC address. According to the application scenario, there are two configuration methods:

- Frame filtering
- MAC address filtering

Frame filtering: Perform filtering operations based on predefined destination MAC addresses or Ethernet frame types. The packet filtering in Table 6-12 is supported.

```
AX3517(slot-1/if-gpon-olt-1/1/1)# mac-filter eth-uni <unild> pre- assign <frame-type> <forward|filter>
```

Key parameters explain are listed in below table.

Field	Value Range	Default Values	Explain	Destination MAC	EtherType
Appletalk	Forward Filter	N/A	Optional, AppleTalk.	FF:FF:FF:FF:FF:FF	0x809B, 0x80F3
Arp	Forward Filter	N/A	Optional, ARP.	FF:FF:FF:FF:FF:FF	0x0806
Bridge-management-inf	Forward Filter	N/A	Optional, Bridge management information.	01:80:C2:00:00:00~ 01:80:C2:00:00:FF	
IPv4-broadcast	Forward Filter	N/A	Optional, IPv4 broadcast.	FF:FF:FF:FF:FF:FF	0x0800
IPv4-multicast	Forward Filter	N/A	optional, IPv4 multicast.	01:00:5E:00:00:00~ 01:00:5E:7F:FF:FF	
IPv6-multicast	Forward Filter	N/A	Optional, IPv6 multicast.	33:33:00:00:00:00~ 33:33:FF:FF:FF:FF	
IPx	Forward Filter	N/A	Optional, IPX.	FF:FF:FF:FF:FF:FF	0x8137
netbeui	Forward Filter	N/A	Optional, NetBEUI.	03:00:00:00:00:01	
Pppoe-broadcast	Forward Filter	N/A	Optional, PPPoE broadcast.	FF:FF:FF:FF:FF:FF	0x8863
rarp	Forward Filter	N/A	Optional, RARP.	FF:FF:FF:FF:FF:FF	0x0805

MAC address filtering: Filter packets based on source MAC or destination MAC. Create a MAC address filtering profile

```
AX3517(slot-1)# gpon profile mac-filter id <id1> <id2> name <name>
```

```
<source|destination> <mac-addr> <forward|filter>
```

Apply profile to ONU

```
AX3517(slot-1/if-gpon-olt-1/1/1)# mac-filter eth-uni <unild> profile <id1>
```



Note: According to the definition of the G.988 standard, if the filter entry is configured

as filter, other MAC addresses will be forwarded by default. Correspondingly, if the filter entry is configured as forward, other MAC addresses will be filtered by default. Therefore, to avoid conflicts, do not configure forward and filter at the same time when configuring the profile.

6.5.10 VLAN Configuration

ONU VLAN:

ONT-VLAN command is used to configure VLAN operation based on ONU port

```
AX3517(slot-1/if-gpon-olt-1/1/1)# ont-vlan ethuni <ID> up-mode
```

```
<transparent|overwrite|add-vid> down-mode <transparent|delete-vid> up- pri <pri> up-vid <vid>
```


Port VLAN:

Port-VLAN is used to configure packet-based VLAN operations

Configure global downlink operation rules first, and then configure packet operation rules. For the same UNI port, you can configure multiple packet rules as needed.

```
AX3517(slot-1/if-gpon-olt-1/1/1)# port-vlan <ID> downstream <ds- operation> intpid <tpid> outtpid <tpid>
```

```
AX3517(slot-1/if-gpon-olt-1/1/1)# port-vlan <ID> rule <ruleid>
```

```
<filter-pkt> <filter-tag> <treatment> <treatment-tag> <ether-type>
```

Field	Value Range	Default Values	Explain
ID	1-24,127,128	N/A	Required, UNI port number.
ds-operation	inverse-upstream forward filter-vid-pbit-forward filter-vid-only-forward filter-pbit-only-forward filter-vid-pbit-disacrd filter-vid-only-disacrd filter-pbit-only-disacrd disacrd	N/A	Mandatory, the operation rule in the downstream direction.
Intpid		N/A	Required, the inner TPID value. For Treatment operation is TPID configuration.
outtpid		N/A	Mandatory, the outer TPID value. For Treatment operation is TPID configuration.
ruleid		N/A	Required, the rule ID number.
Filter-pkt	double-tag single-tag untag	N/A	Required, filter packet type.
Filter-outer-tpid	Mode0 Mode4 Mode5 Mode6 Mode7	Mode0	Optional, filter the outer TPID of the packet.
Filter-outer-pri	0-8	8	Optional, filter the outer priority of packets.
Filter-outer-vid	1-4094	N/A	VLAN ID. Optional, filter the outer VLAN ID of the packet.
Filter-inner-tpid	Mode0 Mode4 Mode5 Mode6 Mode7	Mode0	Optionally, filter the inner packet TPID.

Field	Value Range	Default Values	Explain
Filter-inner-pri	0-8	8	Optional, filter the inner layer priority of packets.
Filter-inner-vid	1-4094	N/A	Optional, filter the inner VLAN ID of the packet.
Treatment	Discard q-in-q remove-tag translate transparent	N/A	Required, operation type.
Treatment-inner-tpid	Mode0 Mode1 Mode2 Mode3 Mode4 Mode6 Mode7	Mode0	Optional, inner TPID.
Treatment-inner-pri	0-7, copy	Copy	Optional, inner priority.
Treatment-inner-vid	1-4094	4096	Optional, inner VLAN ID.
Treatment-outer-tpid	Mode0 Mode1 Mode2 Mode3 Mode4 Mode6 Mode7	Mode1	Optional, outer TPID.
Treatment-outer-pri	0-7, copy	Copy	Optional, outer priority.
Treatment-outer-vid	1-4094	4096	Optional, the outer VLAN ID.
Ether-type	0-5	0	Optional, filter the Ethernet type of packets.

6.5.11 ONU Upgrade

AX3517/AX3515/AX3508/AX3502 provides CLI commands to upgrade ONU. Support two modes to upgrade ONU:

【Configuration prerequisites】

- Confirm that the ONU upgrade file has been uploaded to the OLT Flash /tftpboot/ directory.
AX3517# download ip <ip> src <filename> dst /tftpboot/<filename>
- Check the ONU Equipment ID and Vendor Product Code through the command
brief-show slot <slot ID> interface gpon-olt 1/1 ont 1 brief.

6.5.11.1 Manual Upgrade

- Enter ONU upgrade configuration mode:

```
AX3517(slot-1)# ont-upgrade
```

- Perform an upgrade

```
AX3517(config-t-ont-ugp)# manual-upgrade 1/1/1 filename <filename> equip-id  
<"equip-id">
```



Note: If a third-party ONU is used, **<equip-id>** must be entered, and the "Equipment ID" can be viewed using the command **brief-show interface gpon-olt 1/1 ont 1 brief**.

- View upgrade configuration and results

```
AX3517#brief-show slot 1 interface gpon-olt 1/1 ont-upgrade-config  
AX3517#brief-show slot 1 interface gpon-olt 1/1ont-upgrade-status
```

6.5.11.2 Automatic Upgrade

- Enter the upgrade configuration mode configuration, configure the FTP server, upgrade file name, ONU type.

```
AX3517(Slot-1)# ont-upgrade
```

```
AX3517(Slot-1/ont-upgrade)# auto-upgrade 1/1 start <start-time> end <stop-time>  
filename <filename> equip-id <equipment-id>
```

The configuration in the following example means that the upgrade starts at 1:00 and ends at 5:00.

```
AX3517(Slot-1/ont-upgrade)# auto-upgrade 1/1 start 1 end 5 filename <filename> equip-id  
<equipment-id>
```



Note: If a third-party ONU is used, **<equip-id>** must be entered, and the "Equipment ID" can be viewed using the command **brief-show interface gpon-olt 1/1 ont 1 brief**.

- View upgrade configuration and results.

```
AX3517#brief-show slot 1 interface gpon-olt 1/1 ont-upgrade-config AX3517#brief-show slot 1  
interface gpon-olt 1/1 ont-upgrade-status
```

6.5.12 ONU Port-Isolate

- Enter the ONU port isolation, enable or disable port isolation

```
AX3517(Slot-1/if-gpon-olt-1/1/1)# port-isolate port-id <physical- port-no> mode <enable|disable>
```

- No port isolation port isolation

```
AX3517(Slot-1/if-gpon-olt-1/1/1)# no port-isolate [port-id  
<physical-port-no>]
```

- View port isolation port isolation

```
AX3517(Slot-1/if-gpon-olt-1/1/1)# show interface gpon-olt <1/port-no> ont <ont-id> port-isolate [port-id <physical-port-no>]
```

Port-id is the UNI number, which is a required parameter of the command. The parameter value is filled in <physical-port-no>, the range is 0-255; 0 represents all ports. If mode with port-id 0 is already configured, you cannot configure any command with a port-id other than 0; you must first restore the port-id to its default value and then set the mode with a port-id other than 0. If a port-id other than 0 is already configured, you cannot configure any command with a port-id of 0; you must first restore all the current port-id non-0 to the default value and then set the port-id to 0.

The optional parameter mode is used to configure whether port isolation is enabled on UNI port <physical-port-no>. The limit is set to enable or disable, and the default value is disable.

6.5.13 ONU Unknown Multicast Configure

1. Enter the ONU configuration, Configure unknown multicast transparent or discard

```
AX3517(Slot-1/if-gpon-olt-1/1/1)# unknown-mc-trans port-id <physical-port-no> method <transparent|discard>
```

2. No Unknown multicast configuration

```
AX3517(Slot-1/if-gpon-olt-1/1/1)# no unknown-mc-trans [port-id <physical-port-no>]
```

3. View unknown multicast configurations

```
AX3517#brief-show slot 1 in g <1/port-no> ont <ont-id> unknown-mc-trans [port-id <physical-port-no>]
```

port-id is the UNI number, which is a required parameter of the command. The value of the parameter is set to <physical-port-no>, which ranges from 0 to 255. 0 represents all ports. If you have already configured a method with port-id 0, you cannot configure any command with a port-id other than 0; you must first restore the port-id to its default value and then set the method with a port-id other than 0. If you have already set a port-id other than 0, you cannot configure any command with a port-id of 0; you must first restore all the current port-id non-0 to the default value and then set the method with a port-id of 0.

The optional parameter method is used to configure whether UNI port <physical-port-no> enables unknown multicast passthrough, and the limit is filled in transparent or discard. The default value is discard.

6.6 FEC

The PON system supports bidirectional forward error correction (FEC). By default, FEC is activated. By default, the ONU supports downlink adaptive reception.

- Configure FEC

```
AX3517(slot-1)#interface gpon-olt 1/1
```

```
AX3517(slot-1/if-gpon-olt-1/1)# fec-tx
```

```
AX3517(slot-1/if-gpon-olt-1/1)# ont 1
```

```
AX3517(slot-1/if-gpon-olt-1/1)# fec-tx
```

- Check FEC configuration
AX3517(slot-1/if-gpon-olt-1/1/1)# brief-show configuration running
- Turn off the FEC function
AX3517(slot-1)# interface gpon-olt 1/1
AX3517(slot-1/if-gpon-olt-1/1)# no fec-tx
AX3517(slot-1/if-gpon-olt-1/1)# ont 1
AX3517(slot-1/if-gpon-olt-1/1/1)# no fec-tx

6.7 Encryption

The PON system supports broadcast transmission of downlink services, and malicious users can easily capture information of other users. This leads to two major security problems for PON network systems: the user's information is eavesdropped (user problem), and the other is service theft (service provider problem). In order to prevent the downlink transmission from being eavesdropped, the AX3517/AX3515/AX3508/AX3502 system provides downlink AES algorithm encryption

Advanced Encryption Standard--AES

According to the user's request, the communication between the ONU and the OLT can be encrypted communication.

- Enter the OLT configuration mode to configure and enable PON encryption.
AX3517(slot-1)# interface gpon-olt 1/1
AX3517(slot-1/if-gpon-olt-1/1)# key-exchange-ctrl <enable|disable> AX3517(slot-1/if-gpon-olt-1/1)# key-exchange-interval <interval>
key-exchange-interval:Key exchange timer, used to automatically reset the key.
- Check the PON encryption configuration.
AX3517(slot-1/if-gpon-olt-1/1)# brief-show slot 6 interface gpon- olt 1/1 key-exchange-control
AX3517(slot-1/if-gpon-olt-1/1)# brief-show slot 6 interface gpon- olt 1/1 key-exchange-interval
- Enter ONU configuration mode and configure single GEM Port encryption.
AX3517(slot-1)# interface gpon-olt 1/1
AX3517(slot-1/if-gpon-olt-1/1)# ont 1
AX3517(slot-1/if-gpon-olt-1/1/1)# virtual-port <vportId> encrypt
<disable|bidirection|downstream>
- Check the ONU encryption configuration.
AX3517(slot-1/if-gpon-olt-1/1)# show interface gpon-olt 1/1 ont 1 virtual-port 1

6.8 PON Protection

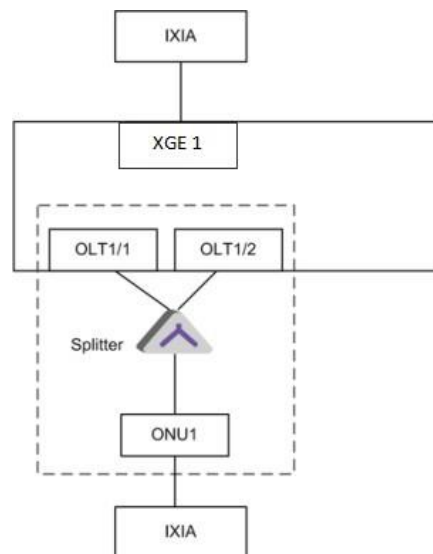
6.8.1 Protection Between PON Ports

To protect the network connection from the failure of the PON port and the optical fiber between the PON port and the splitter, the AX3517/AX3515/AX3508/AX3502 implements the PON protection function.

6.8.1.1 Application Description

Realize group protection between OLT 1/1 and OLT 1/5 of AX3517/AX3515/AX3508/AX3502.

6.8.1.2 Topology Example



In the above topology example below figure, PON1/1 and PON1/5 are protection groups. Use a 2:N optical splitter (optical splitter has two upstream ports and N downstream ports).

6.8.1.3 Operating Steps

- Configuring PON Protection
 - 1) Enter PON protection configuration command mode
AX3517(slot-1)# interface pon-protection-group 1
 - 2) Activate the PON protection function of group 1 in slot 1
AX3517(config-pon-protection-grp-1)# member-ports 1/1 1/5 typeB
AX3517(config-pon-protection-grp-1)# exit
 - 3) View PON Protection
AX3517(slot-1)# show interface pon-protection-group

- Configuring ONU registration and services



Note: After the protection group takes effect, the configuration on the two protection

ports will be automatically cleared. After that, both the Work port and the Protect port can be configured, and the system will automatically synchronize the configuration.

- 4) Enter the Work OLT port configuration command mode.

```
AX3517(slot-1)# interface gpon-olt 1/1
```

```
AX3517(slot-1/if-gpon-olt-1/1)#
```

- 5) Enter the ONU configuration command mode and configure the binding between ONU ID and SN.

```
AX3517(slot-1/if-gpon-olt-1/1)# ont 1
```

```
AX3517(slot-1/if-gpon-olt-1/1/1)# sn GPON005F31A1
```

For details about ONU service configuration, see "[Configuring ONU Service](#)".

- Manual conversion between active and redundant ports

- 1) Enter PON protection configuration command mode

```
AX3517(slot-1)# interface pon-protection-group 1
```

- 2) Switch the active port.

```
AX3517(config-pon-protection-grp-1)# manual-switch w2p
```

```
AX3517(config-pon-protection-grp-1)# exit
```

```
AX3517(slot-1)#
```

- Delete a PON protection group 1)Enter configuration mode

```
AX3517(slot-1)# no interface pon-protection-group 1
```

```
AX3517(config-pon-protection-grp-1)# member-ports 1/1 1/5 typeB AX3517(config-pon-protection-grp-1)# exit
```

6.8.2 Cross-frame PON Protection

In order to protect the network connection from OLT failures, OLT implements the cross-frame PON protection function, and the two PON ports are distributed on different OLT, which can be distributed in the same room or in different rooms

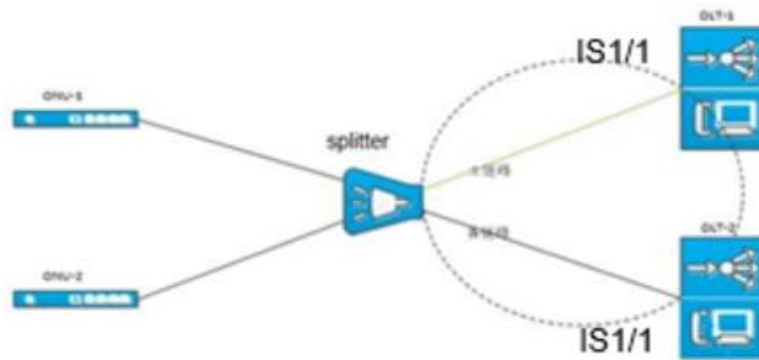
6.8.2.1 Application Description

Group protection between OLT primary 1/1 and OLT standby 1/1 is implemented.



Note: The slots and ports of the main and backup line cards should be consistent.

6.8.2.2 Application Description



6.8.2.3 Operating Steps

The tasks for configuring PON protection are as follows:

1. Configure PON protection
2. Configure ONU registration and service
3. Dual homing operation command

6.8.2.4 Configure Cross-Frame PON Protection

OLT-1 (primary):

```
AX3517#configure pon-protection-group 1 dual-homing local-member 1/1
```

```
peer-member 1/1 local-role work
```

```
AX3517#dual-homing name 17 peer-ip 192.168.7.101 local-ip
```

```
192.168.7.102
```

OLT-2 (standby):

```
AX3517#configure pon-protection-group 1 dual-homing local-member 1/1 peer-member
```

```
1/1 local-role standby
```

```
AX3517#dual-homing name 17 peer-ip 192.168.7.102 local-ip
```

```
192.168.7.101
```

6.8.2.5 Configure ONU Registration and Services

Note: After the protection group is in effect, the configuration on the two protection ports will be automatically cleared. After that, both the Work port and the Protect port can be configured, and the system will automatically synchronize the configuration.

1. Enter the Work OLT port configuration command mode

```
AX3517(Slot-1)# interface gpon-olt 1/1
```

```
AX3517(Slot-1/if-gpon-olt-1/1)#
```


2. Enter the ONU configuration command mode to configure the binding of ONU ID and SN

```
AX3517(Slot-1/if-gpon-olt-1/1)# ont 1
```

```
AX3517(Slot-1/if-gpon-olt-1/1/1)# sn GPON005F31A1 type gpon
```

For specific ONU service configuration, see "Configuring ONU Service Flow"

6.8.2.6 Configure ONU Registration and Services

1. Enter PON Protection configuration command mode

```
AX3517#configure pon-protection-group 1
```

2. Switching active ports

```
AX3517(CONFIG/protect-group-1)# manual-switc
```

3. Batch switching of PON protection groups

```
AX35001#configure manual-switch-range 1-4
```

6.8.2.7 View the Handover Log and the Protection Group Status

1. View handover log

```
AX3517#brief-show pon-protection-log [slotid]
```

2. Check the protection group status

```
AX3517#brief-show pon-protection-group [group id]
```

6.8.2.8 Freeze Protection Group

In the cross-frame PON protection environment, it may be necessary to run in a single frame. Enable the freeze protection group function, and the protection group state is not switched, and the device is restarted in the work state. The frozen state is only

```
AX3517#configure pon-protection-group 1 freeze [enable/disable]
```

6.9 PON Optical Power Monitor

When an optical module with optical power measurement function is inserted into the AX3517/AX3515/AX3508/AX3502, the optical power measurement of the OLT port can be performed. When an optical module with optical power measurement is configured on the ONU, the optical power measurement of the ONU can be performed.

The OLT supports the measurement function of the uplink average optical power it receives from each ONU. When the upstream optical power received by the OLT from an ONU is too low (lower than the upper limit of the OLT sensitivity specified by the standard) or too high (higher than the lower limit of the overloaded optical power of the OLT specified by the standard), the OLT should generate the corresponding optical power over Limit alarms.

The OLT supports querying ONU optical module information. The OLT initiates a query of the optical module information of the ONU through the OMCI message, and the ONU returns the detection result to the OLT.

Based on the measurement of the upstream optical power of the ONU under the PON interface, the OLT can realize the fault diagnosis of the optical link. Fault diagnosis refers to analyzing whether the optical link attenuation and other indicators are

normal according to the optical power of each ONU received on the PON interface, and providing a certain link fault judgment function.

The OLT provides monitoring of parameters such as operating temperature, supply voltage, bias current, and transmitted power of its optical module.

The interface parameters of PON optical power detection are defined as follows:

- Optical temperature of the optical module: expressed as a 16-bit signed binary number, the unit is 1/256 degrees Celsius. Indicates that the range is -128°C to +128°C, and the measurement accuracy should be better than $\pm 3^{\circ}\text{C}$.
- The power supply voltage of the optical module: expressed as a 16-bit unsigned integer (0~65535), the unit is 100 microvolts, the range is 0~6.55 volts, and the measurement accuracy should be better than $\pm 3\%$. This parameter refers to the power supply voltage of the optical transmitter.
- Optical transmitter bias current: expressed as a 16-bit unsigned integer (0 ~ 65535), the unit is 2 microamps, the range is 0 ~ 131 mA, and the measurement accuracy should be better than $\pm 10\%$.
- Optical transmitter output power: expressed as a 16-bit unsigned integer (0 ~ 65535), the unit is 0.1 microwatt (uW), the representation range is 0-6.5535 mW (about -40dBm ~ +8.2 dBm), measurement accuracy Should be better than $\pm 3\text{dB}$.
- Received optical power of the optical receiver: the average optical power received by the OLT from each online ONU, expressed as a 16-bit unsigned integer (0 ~ 65535), the unit is 0.1 microwatt (uW), and the range is 0~6.5535 mW (approximately -40dBm ~ +8.2 dBm), the measurement accuracy in the range of -30dBm to -10dBm should be better than $\pm 1\text{dB}$.

6.9.1 PON Port Optical Power

Use the following command to display the parameters of the optical power diagnostic detection interface of the OLT:

```
AX3517(slot-1)# brief-show slot 15 interface gpon-olt 1/1 optical- info
```

```
Power Feed Voltage(V)      : 3.34
```

```
Optical Launch Power(dBm) : 4.0097
```

```
Laser Bias Current(mA)     : 5.762
```

```
Temperature(Centigrade)    : 37.94
```

```
AX3517(slot-1)#
```

Use the following command to detect the received optical power of the OLT for a specific ONU:

```
AX3517(slot-1)# sbrief-show slot 15 interface gpon-olt 1/1 optical-info ont 1 received-power
```

6.9.2 ONU Optical Power

Run the following commands to query the optical module information of the ONU:

```
AX3517(slot-1)# brief-show slot 15 interface gpon-olt 1/1 ont 1 optical-info
```

```
Power Feed Voltage(V) :3.26
```

```
Received Optical Power(dBm) :-14.3300
```

```
Optical Launch Power(dBm) :2.0460
```

```
Laser Bias Current(mA) :19.850
```

```
Temperature(Centigrade) :40.67
```

6.9.3 Optical Monitor

Run the following commands to set the optical power alarm threshold of the OLT:

```
AX3517(slot-1)# olt-opm
```

```
AX3517(slot-1/config-t-olt-opm)# control port-list 1/1 AX3517(slot-1/config-t-olt-opm)# control  
ont-list 1
```

```
AX3517(slot-1/config-t-olt-opm)# control start-time <hh:mm> AX3517(slot-1/config-t-olt-opm)#  
control period <The unit is 10s> AX3517(slot-1/config-t-olt-opm)# control status <enable|disable>
```

```
AX3517(slot-1/config-t-olt-opm)# alarm <Alarm ID> threshold <Raise Threshold> <Clear Threshold>
```

6.10 Rogue ONU Detection

Since the GPON system adopts time division multiplexing technology in the upstream direction, all ONUs must emit light in the time slot designated by the OLT to make the GPON system work normally. ONUs that do not emit light in the time slot designated by the OLT, such as long light, random light, and light leakage ONUs It will cause upstream signal conflict, and affect other ONUs under the same PON port from time to time, failing to register, or going online and offline repeatedly. Such ONUs are collectively referred to as rogue ONUs.

The AX3517/AX3515/AX3508/AX3502 system supports detecting whether there is a rogue ONU in the system, and locates and isolates it. Help with troubleshooting.

Configure rogue ONU detection with the following command:

```
AX3517(slot-1)# anti-rogueont <port ID> <enable|disable>  
<manual|auto>
```

View rogue ONU detection configuration:

```
AX3517(slot-1)# show anti-rogueont
```



Note: "Manual" mode reports an alarm after locating a rogue ONU, and the user

decides whether to turn off the ONU light. In "Auto" mode, after locating a rogue ONU, it reports an alarm and automatically turns off the ONU light. Due to the complexity of the optical path environment, misjudgment may occur in ONU positioning. It is recommended to perform manual operations during troubleshooting.

AX3517(slot-1/if-gpon-olt-1/1/1)# rogue-ont disable

When using Auto mode, after locating a rogue ONU, the ONU light will be automatically turned off, marked as a rogue *ONU*, and the ONU registration will be rejected. If the ONU returns to normal (after the ONU is normally lighted, it is not in a long light-emitting state), you need to use the following CLI commands Allow this ONU to re-register.

AX3517(slot-1/if-gpon-olt-1/1/1)# rogue-ont enable



Note: Rogue ONU detection is a debugging method for troubleshooting. After troubleshooting, manually disable the rogue ONU detection function to avoid affecting normal business.

6.11 EasyPON

This feature configures a three-mode module to a dual-mode/single-mode mode, or a dual-mode module to a single-mode mode

AX3517(Slot-10/if-gpon-olt-1/1)#pon-port-mode gpon

AX3517(Slot-10/if-gpon-olt-1/1)#pon-port-mode xg-pon-combo

Parameter	Description
gpon	Only the gpon ONU can be found
xg-pon	Only the xgpon ONU can be found
xgs-pon	Only the xgspon ONU can be found
xgs-xg-pon	Only the xgspon&xgpon ONU can be found
xg-pon-combo	Only the xgpon&gpon ONU can be found
xgs-pon-combo	Both xgspon&xgpon&gpon ONU can be found

6.12 PON Energy Saving

In the power saving state, the system determines whether to shutdown the port based on service availability.


6.12.1 Automatic Energy Saving

The following example uses slot 10 as an example Config slot energy conservation.

```
AX3517(CONFIG)#autosavepower 1-10 oprstate <enable|disable>
```

Config port energy conservation.

```
AX3517(CONFIG)#autosavepower 1-10 port 1 oprstate <enable|disable>
```

 **Note:** Shelf-Slot ranges from 1-17 , A, and B.

6.12.2 Manual Energy Saving

The following example uses slot 10 as an example Config slot energy conservation.

```
AX3517(CONFIG)#manualsavepower 1-10 oprstate <up|down|savepower>
```


Enable port energy conservation.

```
AX3517(CONFIG)#manualsavepower 1-10 port 1 oprstate
```

```
<up|down|savepower>
```

6.13 ONU Automatic Registration

After this command is enabled, all discovered unregistered ONUs are automatically registered and the configuration is delivered according to the automatic registration template

 **Note:** Before using the automatic registration function, configure an automatic registration template.

6.13.1 Configure Automatic Registration Template


```
AX3517#config gpon-profile ont-template 1
```

- Configure virtual-port

```
AX3517(CONFIG/config-t-gpon-pro/ont-template-1)#virtual-port 1 port unlock
```

- Configure service

```
AX3517(CONFIG/config-t-gpon-pro/ont-template-1)#service flow- profile 2 tcont-bind-profile 1
```

 **Note:** The flow template needs to be configured , AX3517(Slot-10)#gpon profile flow id 2 1 name flow2 uni-type ethernet-uni uni-bitmap 0xf upmap-type vlanId 100 101 pri-bitmap 0xff

- Configure vlan translate

```
AX3517(CONFIG/ont-template-1)#user-service virtual-port 1 svid 101 new-svid 101
```

6.14 Automatically Register and Apply Templates

- Enable automatic registration globally and apply templates to the PON port

```
AX3517(Slot-10)#gpon profile auto-register-model 1 port 1 ont- templateid 1
```

If you specify the onu equip-id application automatic registration template, you can deliver different preconfiguration templates to different onu models

```
AX3517(Slot-10)#gpon profile auto-register-model 1 port 1 ont- templateid model-type equip-id  
equipment <equipment id>
```

- Automatic registration is enabled in the PON port and template is applied

```
AX3517(Slot-10/if-gpon-olt-1/1)#auto-register ont-template 1
```

- Configure onu equip-id to deliver the specified automatic registration template

```
AX3517(Slot-10/if-gpon-olt-1/1)#auto-register-model 1 ont- templateid 1 model-type equip-id  
equipment <equipment id>
```

6.14.1 Automatic Registration Aging

If this function is enabled, the device automatically deletes the automatically registered onu when the disconnected time reaches the specified aging time.

```
AX3517(CONFIG)#ont-mngt auto-agingtime 6h
```



Note: After the active/standby switchover or restart of the device, the aging time is reset.

6.14.2 Automatically Registering for Migration



Note: Before configuration, ensure that automatic registration is enabled for ports before and after migration

After this function is enabled, if the onu that is automatically registered with port 1 is migrated to port 2, the onu automatically delivers an automatic registration template and deletes the onu of port 1

Enable auto-migration

```
AX3517(CONFIG)#ont-mngt auto-migration enable
```

Disable auto-migration

```
AX3517(CONFIG)#ont-mngt auto-migration disable
```

6.15 ONU WAN port configuration or Wi-Fi configuration

Configure WAN IP

```
AX3517(Slot-1/if-gpon-olt-1/1/1)#wan-ip 1 ipv4 1.2.3.4
```

```
255.255.255.0 1.2.3.1 static
```

Configure wan-ip-cfg

```
AX3517(Slot-1/if-gpon-olt-1/1/1)#wan-ip-cfg id 1 ip-addr 1.2.3.4
```

```
255.255.255.0 1.2.3.1 pri-dns 10.10.10.1 sec-dns 10.10.10.2
```

Configure wan service

```
AX3517(Slot-10/if-gpon-olt-1/1/1)#ont-wan-config wan-id <1..16> mode <bridge/route> vlan  
<0..4094> service-mode <0..7> port-bind <0x*>
```



Note: service-mode <0..7>Parameter Description:

```
<other(0)|internet(1)|voip(2)|voip_internet(3)|tr069(4)|tr069_internet(5)|tr069_voip  
_internet(7)>.
```

```
<0x*>:'0x',0 means no bind, port bind bitmap(port1:0x1 port2:0x2 port3:0x4 port4 :0x8 port5 :0x10)
```

Configure the number of wan services

```
AX3517(Slot-10/if-gpon-olt-1/10/1)#ont-wan-config wan-number 1
```

Configure the onu WIFI service in WEP mode

```
AX3517(Slot-10/if-gpon-olt-1/1/1)#ssid-auth 1 auth WEP open-system password
```

```
key-104 keyword1
```

Configure the onu WIFI service in WPA-PSK mode

```
AX3517(Slot-10/if-gpon-olt-1/1/1)#ssid-auth 1 auth WPA WPA-PSK password
```

```
12345678
```

6.16 ONU SNTP

Deliver information about the onu active and standby clock servers and the time zone

```
AX3517(Slot-10/if-gpon-olt-1/1/1)#sntp time-zone GMT+12:00 master- server 10.10.10.1 slave-server
```

```
10.10.10.10.2 interval 10
```

7 Multicast Configuration

Multicast is used to support real-time applications such as video conferencing and streaming audio. The multicast server does not need to establish a separate connection with each client, but simply transmits services to the network. A host that wants to receive multicast services must register with its local multicast switch / router.

AX3517/AX3515/AX3508/AX3502 supports Layer 2 and uses the following protocols:

IGMP snooping (layer 2)

7.1 IP Multicast Introduction

The multicast IP address is Class D IP address, ranging from 224.0.0.0 to 239.255.255.255.

Some of the multicast IP addresses listed below are reserved for special purposes.

- 224.0.0.1: All hosts available for multicast
- 224.0.0.2: All multicast routers
- 224.0.0.4: All DVMRP routers
- 224.0.0.5: All OSPF routers
- 224.0.0.13: All PIM routers

Normally, addresses from 224.0.0.1 to 224.0.0.255 are reserved for other protocols.

Control VLAN: Configure the VLAN to transmit IGMP messages, such as report messages, query messages, etc.

Business VLAN: Configure this VLAN to transport business packets, such as IPTV data.

7.2 IGMP Snooping Introduction

AX3517/AX3515/AX3508/AX3502 can use IGMP (Internet Group Management Protocol, Internet Group Management Protocol) snooping to suppress the flooding of multicast services. By dynamically configuring ports, multicast services are only forwarded to those related to IP multicast devices port.

IGMP snooping requires LAN switches to monitor IGMP traffic between hosts and routers, and keep track of multicast groups and member ports.

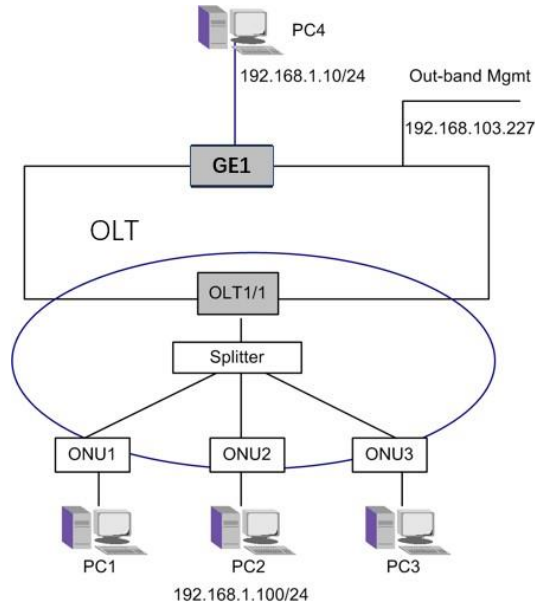
Layer 2 multicast entries are learned through IGMP snooping.

7.3 IGMP Configuration Instance

7.3.1 Application Description

In the application example shown in [IGMP Snooping configuration](#), the PCs connected to ONU1, ONU2, and ONU3 all receive multicast services. IGMP configuration is illustrated using the following example.

7.3.2 Topological Instance



In above figure, the AX3517/AX3515/AX3508/AX3502 is connected to the multicast source PC4 through the XGE1 upstream port. Downstream ports OLT1/1 are connected to ONU1, ONU2 and ONU3 through optical splitters. Ports XGE1, IS1/1 and all ONUs belong to VLAN101. PC1, PC2 and PC3 are respectively connected to their corresponding ONUs (ONU1-3). PC1-3 are all multicast group members and receive multicast services from AX3517/AX3515/AX3508/AX3502.

When connecting a new downstream user to a certain group, the user sends an IGMP membership report message. The report message is received and snooped by AX3517/AX3515/AX3508/AX3502. After the entry is added, the IGMP report message is forwarded to the upstream device.

In this example, PC4 sends multicast services. Three PCs 1-3 receive multicast services.

7.3.3 Configuration Requirements

- Take a home gateway ONU as an example, the WAN configuration of ONU1, ONU2 and ONU3 is in bridge mode, and the VLAN ID is 101. For details, see the "ONU Configuration Manual".
- ONU1, ONU2, and ONU3 bind to the corresponding ONU ID, respectively.
- The installation of the multicast source application of the multicast source PC4 is completed.

7.3.4 The task list of configuration

- Create multicast VLAN
- Enable IGMP Snooping
- Configure ONU multicast profile
- Check IGMP

7.3.4.1 Create multicast VLAN

- Create a multicast VLAN 4000-4003, configure XGE1, and configure IS1/1 as a tagged member port.
- Create unicast VLAN 101 and configure XGE1 as the tagged member port of this VLAN.
- Create VLAN 3800 for mapping to the multicast GEM port as a tagged member of this VLAN. Please refer to VLAN configuration.
- Configure unicast VLAN translation.

```
AX3517(CONFIG/L2/VLAN)# translate slot 1 port 1 ont 1 virtual-port
```

```
1 svid 101 new-svid 101
```

```
AX3517(CONFIG/L2/VLAN)# translate slot 1 port 1 ont 2 virtual-port
```

```
1 svid 101 new-svid 101
```

```
AX3517(CONFIG/L2/VLAN)# translate slot 1 port 1 ont 3 virtual-port
```

```
1 svid 101 new-svid 101
```

7.3.4.2 Enable IGMP-Proxy

- Enter the multicast configuration mode.

```
AX3517(CONFIG)# multicast
```
- Configure IGMP mode.

```
AX3517(CONFIG/MCAST)# multicast-handling snooping-with-proxy
```
- Configure multicast VLAN information.

```
AX3517(CONFIG/MCAST)# group-to-vlan 1 4000 225.0.0.1 225.0.0.10
```
- Configure the mapping from multicast VLAN to GEM Port.

```
AX3517(CONFIG/MCAST)# vlan-to-gem 1 4000 4003 3800
```

7.3.4.3 Enable IGMPv3-Proxy

- Enter the multicast configuration mode.

```
AX3517(CONFIG)# multicast
```
- Configure IGMP mode.

```
AX3517(CONFIG/MCAST)# multicast-handling snooping-with-proxy
```
- Configure IGMPv3 mode.

```
AX3517(CONFIG/MCAST)# parameter igmp-version 3
```

- Configure multicast VLAN information.

```
AX3517(CONFIG/MCAST)# group-to-vlan 1 4000 225.0.0.1 225.0.0.10
```

- Configure the mapping from multicast VLAN to GEM Port.

```
AX3517(CONFIG/MCAST)# vlan-to-gem 1 4000 4003 3800
```

7.3.4.4 Configure ONU Multicast Profile

- Configuring a Multicast Action profile

```
AX3517(slot-1)# gpon profile multicast-oper id 1 name mop_1 igmp- ver v3 ctrl-mode snooping-only  
fastleave enable
```

- Configure the dynamic multicast profile.

```
AX3517(slot-1)# gpon profile multicast-dynamic id 1 1 name mcast_1 gemport 3800 vlanid 4000 srcip  
192.168.1.10 grpaddr-start 225.0.0.1 grpaddr-stop 225.0.0.10 grpbw 1000
```

```
AX3517(slot-1)# gpon profile multicast-dynamic id 2 1 name mcast_1 gemport 3800 vlanid 4001 srcip  
192.168.1.10 grpaddr-start 225.0.0.1 grpaddr-stop 225.0.0.10 grpbw 1000
```

```
AX3517(slot-1)# gpon profile multicast-dynamic id 3 1 name mcast_1 gemport 3800 vlanid 4001 srcip  
192.168.1.10 grpaddr-start 225.0.0.1 grpaddr-stop 225.0.0.10 grpbw 1000
```

- Configure the dynamic v6 multicast profile.

```
AX3517(Slot-1)# gpon profile multicast-dynamic id 1 2 name mcast_1 gemport 3800 vlanid 4000  
grpipv6addr-start ff1e::1 grpipv6addr-stop ff1e::10
```

The key parameters are described in the following tables:

ONU Multicast Operating profile Parameter Column Chart

Field	Value Range	Default Values	Explain
lgmp-ver	v1	N/A	Required, IGMP protocol version.
	v2		
	v3		
ctrl-mode	snooping-only	N/A	Mandatory, multicast protocol type.
	snooping-with-proxy		
	proxy-reporting		
Fast-leave	enable	N/A	Required, whether to enable quick leave.
	disable		
us-tag-ctrl	pass	Pass	Optional, VLAN tag operation of upstream IGMP protocol packets.
	add		
	replace		
	rep-vid-only		
us-tci-pbits	0~7	0	Optional, the Priority value of the upstream IGMP protocol packet, which takes effect only when "us-tag-ctrl" is add/replace.

Field	Value Range	Default Values	Explain
us-tci-vlanId	0~4095	0	Optional, VLAN ID value of upstream IGMP protocol packets, only valid when "us-tag-ctrl" is add/replace/rep-vid-only.
ds-tag-ctrl	Pass strip add replace rep-vid-only	Pass	Optional, VLAN tag operation of downstream multicast packets.
ds-tci-pbits	0~7	0	Optional, the Priority value of downlink multicast packets, which takes effect only when "ds-tag-ctrl" is add/replace.
ds-tci-vlanId	0~4095	0	Optional, VLAN ID value of downlink multicast packets, only valid when "ds-tag-ctrl" is add/replace/rep-vid-only.

ONU Dynamic Multicast profile Parameter Column Chart

Field	Value Range	Default Values	Explain
Gemport	3800~3999(GPON) 4568~4767(XGPON/XGSPON)	N/A	Mandatory, multicast GEM Port.
vlanid	1~4094	N/A	Required. Multicast VLAN.
Src-ip	0.0.0.0~255.255.255.255	N/A	Mandatory, the multicast source IP address.
grpaddr-start	224.0.0.0~255.255.255.255	N/A	Mandatory, the start address of the multicast group.
grpaddr-stop	224.0.0.0~255.255.255.255	N/A	Mandatory, the end address of the multicast group.
grpbw	0~10000000	0	The maximum imputed dynamic bandwidth. The unit is kbps.

- Configure flow profiles.

```
AX3517(slot-1)# gpon profile dba id 1 name dba_1 type4 max 1244160 AX3517(slot-1)#
```

```
gpon profile tcont-svc id 1 name tcont_1 dba-id 1
```

```
AX3517(slot-1)# gpon profile flow id 1 1 name flow_1 uni-type eth- uni uni-bitmap 0xf upmap-type vlanId 101 101 pri-bitmap 0xff vport 1
```

```
AX3517(slot-1)# gpon profile vportsvc id 1 name vp_svc_1 encry- mode disable us-pri 0
```

```
usratectrl-id 0 dsratectrl-id 0
```

```
AX3517(slot-1)# gpon profile tcont-bind id 1 v-port 1 name 1 vportsvc-id 1 tcont-id 1 tcontsvc-id
```

1

- Apply the profile to ONU 1, ONU 2, and ONU 3 operates similarly, example is for ONU1, apply multicast VLAN 4000 to UNI port 1-2, multicast VLAN 4001 to UNI port 3, multicast VLAN 4002 to UNI port 3.

```
AX3517(slot-1)# interface gpon-olt 1/1 AX3517(slot-1/if-gpon-olt-1/1)# ont 1
```

```
AX3517(slot-1/if-gpon-olt-1/1/1)# virtual-port 1 port unlock
```

```
AX3517(slot-1/if-gpon-olt-1/1/1)# service flow-profile 1 tcont- bind-profile 1
```

```
AX3517(slot-1/if-gpon-olt-1/1/1)# multicast eth-uni 1 oper-profile
```

```
1 dynamic-profile 1
```

```
AX3517(slot-1/if-gpon-olt-1/1/1)# multicast eth-uni 2 oper-profile
```

```
1 dynamic-profile 1
```

```
AX3517(slot-1/if-gpon-olt-1/1/1)# multicast eth-uni 3 oper-profile
```

```
1 dynamic-profile 2
```

```
AX3517(slot-1/if-gpon-olt-1/1/1)# multicast eth-uni 4 oper-profile
```

```
1 dynamic-profile 3
```

7.3.4.5 Check IGMP

Send the multicast membership report on PC1 and start the multicast source service on PC4. If PC1 receives a normal multicast stream, it means that IGMP snooping on AX3517/AX3515/AX3508/AX3502 is working.

- View multicast table:

```
AX3517(CONFIG/MCAST)# snooping show multicast-group
```

7.4 Enable MLDv2 Proxy

- Enter the multicast configuration mode

```
AX3517(CONFIG)# multicast
```

- Configure IGMP mode

```
AX3517(CONFIG/MCAST)# multicast-handling snooping-with-proxy
```

- Configure MLDv2 mode

```
AX3517(CONFIG/MCAST)#parameter mld-version 2
```

- Configure multicast VLAN information

```
AX3517(CONFIG/MCAST)# group-v6-to-vlan 1 4000 ff1e::1 ff1e::10
```

7.4.1 Configure ONU Multicast Action Profile

1. Configuring a Multicast Action profile

```
AX3517(Slot-1)# gpon profile multicast-oper id 1 name mop_1 igmp-ver MLDv2 ctrl-mode snooping-only
fastleave enable
```

2. Configure v6 dynamic multicast templates

```
AX3517(Slot-1)# gpon profile multicast-dynamic id 1 1 name mcast_1 gemport 3800 vlanid 4000
grpipv6addr-start ff1e::1 grpipv6addr-stop ff1e::10
```

The key parameters are described in the following tables.

ONU Multicast Operating profile Parameter Column Chart

Field	Value Range	Default values	Explain
lgmp-ver	v1 v2 v3	N/A	Required, IGMP protocol version.
ctrl-mode	snooping-only snooping-with- proxy proxy- reporting	N/A	Mandatory, multicast protocol type.
Fast-leave	enable disabl e	N/A	Required, whether to enable quick leave.
us-tag-ctrl	pass add replac e	Pass	Optional, VLAN tag operation of upstream IGMP protocol packets.
us-tci-pbits	rep-vid-only 0~7	0	Optional, the Priority value of the upstream IGMP protocol packet, which takes effect only when "us-tag-ctrl" is add/replace.
us-tci-vlanid	0~4095	0	Optional, VLAN ID value of upstream IGMP protocol packets, only valid when "us-tag-ctrl" is add/replace/rep-vid-only.
ds-tag-ctrl	pass strip add replac e rep-vid-only	Pass	Optional, VLAN tag operation of downstream multicast packets.

Field	Value Range	Default values	Explain
ds-tci-pbits	0~7	0	Optional, the Priority value of downlink multicast packets, which takes effect only when "ds-tag-ctrl" is add/replace.
ds-tci-vlanId	0~4095	0	Optional, VLAN ID value of downlink multicast packets, only valid when "ds-tag-ctrl" is add/replace/rep-vid- only.

ONU Dynamic Multicast profile Parameter Column Chart

Field	Value range	Default values	Explain
Gemport	3800~3999(GPON) 4568~4767(XGPON/XGSPON)	N/A	Mandatory, multicast GEM Port.
vlanid	1~4094	N/A	Required. Multicast VLAN.
Src-ip	0.0.0.0~255.255.255.255	N/A	Mandatory, the multicast source IP address.
grpaddr-start	224.0.1.0~239.255.255.255	N/A	Mandatory, the start address of the multicast group.
grpaddr-stop	224.0.1.0~239.255.255.255	N/A	Mandatory, the end address of the multicast group.
grpbw	0~10000000	0	The maximum imputed dynamic bandwidth. The unit is kbps.
grpipv6addr-start	FF00::/32 - FF3F::/32	N/A	Optional, v6 multicast group end address
grpipv6addr-stop	FF00::/32 - FF3F::/32	N/A	Optional, v6 multicast group end address

3. Configure flow template

```

AX3517(Slot-1)# gpon profile dba id 1 name dba_1 type4 max 1244160

AX3517(Slot-1)# gpon profile tcont-svc id 1 name tcont_1 dba- id 1

AX3517(Slot-1)# gpon profile flow id 1 1 name flow_1 uni-type veip uni-bitmap 0xff upmap-type vlanId 101
101 pri-bitmap 0xff vport 1

AX3517(Slot-1)# gpon profile vportsvc id 1 name vp_svc_1 encry-mode disable us-pri 0 usratectrl-id 0
dsratectrl-id 0

AX3517(Slot-1)# gpon profile tcont-bind id 1 v-port 1 name 1 vportsvc-id 1 tcont-id 1 tcontsvc-id 1

```

4. Apply the template to ONU 1, ONU 2, and ONU 3 similarly

```

AX3517(Slot-1)# interface gpon-olt 1/1 AX3517(Slot-1/if-gpon-olt-1/1)# ont 1

AX3517(Slot-1/if-gpon-olt-1/1/1)# virtual-port 1 port unlock

```

```
AX3517(Slot-1/if-gpon-olt-1/1/1)# service flow-profile 1 tcont-bind-profile 1
```

```
AX3517(Slot-1/if-gpon-olt-1/1/1)# multicast veip 127 oper- profile 1 dynamic-profile 1
```

```
AX3517(Slot-1/if-gpon-olt-1/1/1)# exit
```

7.5 Check MLD Proxy

The multicast member report is sent on PC1 and the multicast source service is started on PC4. If PC1 receives a normal multicast stream, MLD proxy on OLT is working

View the multicast table.

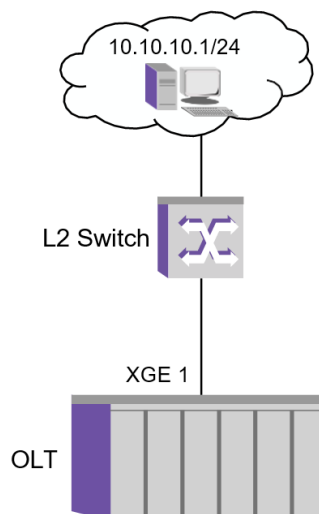
```
AX3517(CONFIG/MCAST)# snooping show mldv2-group
```

8 ACL

ACL (Access Control List) is used to filter data packets, thereby restricting network traffic and restricting network access of specific users or devices. Specific rules are defined in the ACL to allow or deny data packets to access the AX3517/AX3515/AX3508/AX3502 CPU or its designated interface. An ACL is a series of allow and deny conditions applied to incoming packets. When an interface receives a packet, the packet fields are compared with the applied ACL to verify that the packet is allowed to be forwarded. Packets are tested one by one against the list of filter conditions in the ACL.

8.1 Application Description

In the application example shown in below figure. AX3517/AX3515/AX3508/AX3502 is connected to the network through XGE1, and ACL is configured to deny PC (10.10.10.1/24) access to AX3517/AX3515/AX3508/AX3502 through XGE1. Use the following examples to illustrate the ACL configuration.



8.2 Operating Steps

- Creating a Packet Classification Matching Pattern

```
AX3517(CONFIG)# mask srcip priority 1 src-ip 255.255.255.255
```



```
AX3517(CONFIG)# show mask
```

- Creating Traffic Classification Rules

```
AX3517(CONFIG)# rule srcip index 1 mask-priority 1 src-ip 10.10.10.1
```

```
AX3517(CONFIG)# show rule
```

- Create a Flow-Based Security Control

```
AX3517(CONFIG)# security
```

```
AX3517(CONFIG/Security)# action deny acl deny
```

```
AX3517(CONFIG/Security)# show action
```

- Creating a flow-based security configuration

```
AX3517(CONFIG/Security)# assign-action interface xge 1 rule-index
```

```
1 action deny
```

```
AX3517(CONFIG/Security)# show action-assign
```

9 QoS

9.1 Introduction

This section describes how to configure the Quality of Service (QoS) of the AX3517/AX3515/AX3508/AX3502 to select specific network services and prioritize them based on relative importance. Implement QoS in AX3517/AX3515/AX3508/AX3502 to avoid bottleneck congestion, improve network performance predictability and bandwidth utilization.

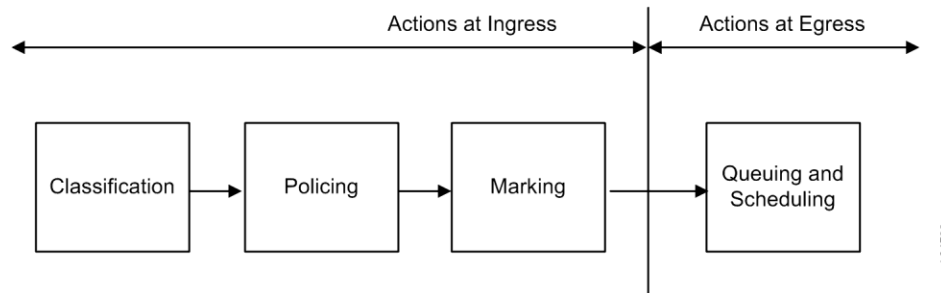
Implementing QoS in the AX3517/AX3515/AX3508/AX3502 provides different priorities for different users and guarantees a certain level of performance to ensure that higher priority services (such as voice and video services) are preferentially processed.

The AX3517/AX3515/AX3508/AX3502 provides the following main QoS features:

- Two configurable QoS modes: 802.1p and DSCP
- Traffic classification
- Traffic policing
- Support for 8 priorities
- Traffic shaping
- Buffer management

QoS operations at the ingress port include classification, policing and marking. The operations at the destination port are queuing and scheduling.

All these functions work together to provide QoS guarantees and fair distribution of excess bandwidth, and to prioritize user traffic (both upstream and downstream directions) between switches and PON systems.



With traffic classification, user frames can be marked in the DSCP field of IP packets or the 802.1p priority field of Ethernet frames.

9.2 Rate Limit

AX3517/AX3515/AX3508/AX3502 provides rate limiting function for upstream and downstream services of XGE ports.

```
AX3517(CONFIG)# qos
```

```
AX3517(CONFIG/QOS)# rate-limit interface <is|xge|trunk> <port> ingress <rate> egress <rate>
```

```
AX3517(CONFIG/QOS)# show rate-limit interface <port>
```

9.3 Queue Mapping

Priority to egress queue mapping.

```
AX3517(CONFIG/QOS)# dot1p-mapping <0..7> queue <0..7>
```

```
AX3517(CONFIG/QOS)# show dot1p-mapping
```

9.4 DSCP Mapping

```
AX3517(CONFIG/QOS)# dscp interface <is|xge|trunk> <port>
```

```
AX3517(CONFIG/QOS)# dscp-mapping interface <xge|trunk|is> <port> ingress-dscp <0..63> new-dscp <0..63>
```

```
AX3517(CONFIG/QOS)# show dscp-mapping
```

9.5 Scheduling Mode

```
AX3517(CONFIG/QOS)# scheduling interface <xge|trunk|is> <port>
```

```
<sp|wrr|wrr+sp>
```

```
AX3517(CONFIG/QOS)# show scheduling
```

9.6 Weight Configuration

```
AX3517(CONFIG/QOS)# scheduling interface <xge|trunk|is> <port>
```

```
<sp|wrr|wrr+sp>
```

```
AX3517(CONFIG/QOS)# show scheduling
```

9.7 Egress Queue Metering

```
AX3517(CONFIG/QOS)# egress-queue-metering interface <xge|trunk|is>
```

```
<port> queue <0..7> <min-cir|max-cir> <range>
```

```
AX3517(CONFIG/QOS)# show egress-queue-metering
```

9.8 Drop Priority Map

```
AX3517(CONFIG/QOS)#ingress-drop-dei interface <xge|trunk|is>
```

```
<port> s-pri <0..7> dei-bit <0|1> precedence <green|yellow|red>
```

```
AX3517(CONFIG/QOS)#ingress-drop-nodei interface <xge|trunk|is>
```

```
<port> s-pri <0..7> precedence <green|yellow|red>
```

```
AX3517(CONFIG/QOS)#drop-precedence interface <xge|trunk|is>
```

```
<port> enable [dei-bit <enable|disable>]
```

9.9 Flow-Based QoS

The configuration task list is as follows:

- Traffic rate limit profile
- Flow-based QoS operation
- Flow-based QoS applied to ports

9.9.1 Traffic Rate Limit Profile

```
AX3517(CONFIG/QOS)# meter <name> type <srtcm|trtcm> cir <cir> pir
```

```
<pir> cbs <pbs> pbs <pbs>
```

9.9.2 Flow-Based QoS Operation

According to different purposes, select the corresponding operation:

```
AX3517(CONFIG/QOS)# action <name> <meter|s-pri|dscp|egress-queue|precedence|traffic-class>
```

```
<name>
```

9.9.3 Flow-Based QoS Applied To Ports

```
AX3517(CONFIG/QOS)# assign-action interface <xge|trunk|is> <port> rule-index <id> action <action-name>
```

10 SyncE

10.1 Introduction

In communication networks, the normal operation of many services requires network time synchronization. Time synchronization includes both frequency and phase synchronization. Through time synchronization, the frequency and phase differences between various devices in the entire network can be kept within a reasonable error range.

Synchronous Ethernet (SyncE) is a synchronization technology that carries and recovers frequency information based on the physical layer code stream. It can achieve high-precision frequency synchronization between network devices, meeting the frequency synchronization requirements of wireless access services. SyncE is usually used in conjunction with PTP technology to simultaneously meet the high-precision requirements of both frequency and phase, achieving nanosecond-level time synchronization. This article mainly introduces the technical principles and typical network applications of SyncE. For an introduction to PTP technology, please refer to the PTP section.

10.2 SyncE Configuration Instance

- Check the uplink port status
- Configure SyncE
- Check the SyncE status of the uplink port

10.2.1 Traffic Metering Profile

- Check the uplink port status, the port needs to be UP.

XGE On	1	Network	Unlock no-FEC	Up	Auto	Auto	Auto	10000M	Full
XGE On	2	Network	Unlock no-FEC	Down	Auto	Auto	Auto	10000M	Full
XGE On	3	Network	Unlock no-FEC	Down	Auto	Auto	Auto	10000M	Full
XGE On	4	Network	Unlock no-FEC	Down	Auto	Auto	Auto	10000M	Full
XGE Off	5	Network	Lock no-FEC	Down	Auto	Auto	Auto	Unknown	Full
XGE Off	6	Network	Lock no-FEC	Down	Auto	Auto	Auto	Unknown	Full
XGE Off	7	Network	Lock no-FEC	Down	Auto	Auto	Auto	Unknown	Full
XGE Off	8	Network	Lock no-FEC	Down	Auto	Auto	Auto	Unknown	Full

10.2.2 Configure SyncE

- Configure the uplink port clock locking priority. Each main control board supports locking one port, and it is recommended to use the default values for SyncE parameters.

```
AX3517#configure clock
```

```
AX3517(CLK)#ethport-clock xge 1 pri 10
```

10.2.3 Check the SyncE status of the uplink port

- Check the SyncE status; "lock" indicates that the frequency has been successfully locked.

```
AX3517(CLK)#show status
```

```
Local SystemLockState      :lock
```

```
Local SCSWorkState         :lock
```

```
Local SCSWorkState_1      :lock
```

```
Local SCSWorkState_2      :lock
```

```
Local SCSWorkState_3      :lock
```

```
Local SCSSelectSource      :XGE 1
```

```
Local SCSSelectSourceSec   :None
```

```
AX3517(CLK)#
```

11 PTP

11.1 Introduction

PTP (Precision Time Protocol) is a protocol for time synchronization that enables high-precision time and frequency synchronization between devices. PTP's time synchronization accuracy is at the sub-microsecond level.

11.1.1 Basic Concepts of PTP

11.1.1.1 PTP Protocol Standard

The PTP protocol standard is also known as the PTP profile. Different types of PTP protocol standards can achieve different PTP functions. The AX3500 series OLT supports IEEE 1588 version 2.

IEEE 1588 version 2: Also known as 1588v2. The IEEE 1588 standard specifies the principles and message interaction protocols for high-precision clock synchronization in networks. It was originally used in industrial automation and is now primarily used for bridging local area networks. IEEE 1588 does not impose strict requirements on the network environment, making it widely applicable and customizable to enhance or trim specific functions according to different application environments. The latest version is V2, or 1588v2.

11.1.1.2 PTP Domain

Network applying the PTP protocol is referred to as a PTP domain. There is one and only one clock source within a PTP domain, and all devices in the domain stay synchronized with this clock.

11.1.1.3 PTP Instance

When a network has multiple types of traffic with different clock synchronization requirements, the network needs to be divided into multiple PTP domains. Devices traversed by the same clock signal are included in the same PTP domain. A PTP instance serves as a PTP parameter configuration template, under which parameters such as the PTP protocol standard and node type can be configured. Different parameters can be configured under different instances. A PTP instance is bound to a PTP domain, and instances are isolated from each other, allowing multiple domains and multiple instances to meet the varying clock synchronization requirements of different types of traffic.

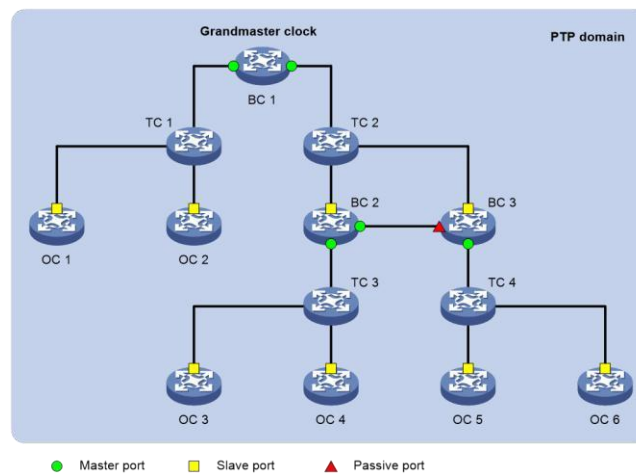
11.1.1.4 Clock Nodes and PTP Interfaces

Nodes within a PTP domain are referred to as clock nodes, and interfaces running the PTP protocol on these nodes are called PTP interfaces. The PTP protocol defines three basic types of clock nodes:

- OC (Ordinary Clock): This clock node has only one PTP interface participating in time synchronization within the same PTP domain, synchronizing time from upstream clock nodes through this interface. Additionally, when the clock node

serves as a clock source, it can publish time to downstream clock nodes through a single PTP interface.

- **BC (Boundary Clock):** This clock node has multiple PTP interfaces participating in time synchronization within the same PTP domain. It synchronizes time from upstream clock nodes through one interface and publishes time to downstream clock nodes through the remaining interfaces. Furthermore, when the clock node acts as a clock source, it can publish time to downstream clock nodes through multiple PTP interfaces, as shown in Connection of RJ-45 / DB9 RS-232 serial port cable figure with BC 1.
- **TC (Transparent Clock):** TC has multiple PTP interfaces but only forwards PTP protocol messages between these interfaces, applying forwarding delay corrections without synchronizing time through any interface. Unlike BC/OC, which must stay synchronized with other clock nodes, TC does not synchronize time with other clock nodes.



11.1.2 Master-Slave Relationship

The master-slave relationship is relative. For a pair of clock nodes that are synchronized, the following master-slave relationship exists:

- **Master/Slave Node:** The clock node that publishes the synchronized time is called the master node, while the clock node that receives the synchronized time is called the slave node.
- **Master/Slave Clock:** The clock on the master node is called the master clock, while the clock on the slave node is called the slave clock.
- **Master/Slave Interface:** The PTP interface on the clock node that publishes synchronized time is called the master port, while the PTP interface that receives synchronized time is called the slave port. Both master and slave ports can exist on BC or OC.

In addition, there is a PTP interface that neither publishes nor receives synchronized time, called the passive port.

In the PTP network, all clock node types (except TC) are connected through a master-slave relationship. The master-slave relationship

between clock nodes can be automatically generated through the BMC algorithm or manually assigned.

11.1.3 Basic Concepts of PTP

As shown in Basic clock nodes figure, all clock nodes within a PTP domain are organized in a hierarchical structure, and the reference time for the entire domain is the optimal clock (Grandmaster Clock, GM), which is the highest-level clock. Clock nodes interact through PTP protocol messages and, based on the information carried in the PTP protocol messages such as clock priority, time level, and clock accuracy, select the optimal clock for the entire PTP domain. The time of the optimal clock will ultimately be synchronized to the entire PTP domain, which is why it is also called the clock source of the PTP domain.

11.1.4 Optimal Clock Election and Master-Slave Relationship Determination

The optimal clock can be manually specified or dynamically elected through the BMC algorithm. The dynamic election process is as follows:

1. Clock nodes exchange Announce messages, and based on the information carried in these messages, such as optimal clock priority, time level, time accuracy, etc., one node is selected as the optimal clock for the PTP domain. At the same time, the master-slave relationship between nodes and the master-slave interfaces on each node are also determined. Through this process, a loop-free, fully connected tree rooted at the optimal clock is established within the entire PTP domain.
2. After this, the master node will periodically send Announce messages to the slave nodes. If, within a certain period of time, the slave node does not receive any Announce messages from the master node, it will consider the master node as failed and will initiate a new optimal clock selection. During the dynamic election of the optimal clock in the PTP domain, each clock node will compare the first priority, time level, time accuracy, and second priority in the Announce messages in sequence. The winner will become the optimal clock.

11.1.5 PTP Synchronization Principle

The basic principle of PTP synchronization is as follows: Once the master-slave relationship between clocks is confirmed, the master and slave clocks exchange PTP protocol messages and record the message sending and receiving times. By calculating the round-trip time difference of the PTP protocol messages, the round-trip delay between the master and slave clocks is calculated. If the transmission delay in both directions is the same, half of the round-trip delay is the one-way delay. The slave clock calculates the time offset based on this one-way delay, the sending time of the Sync message on the master clock, and the time difference between the reception of the Sync message on the slave clock. The slave clock adjusts its local time based on the time offset to achieve synchronization with the master clock.

The PTP protocol defines two transmission delay measurement mechanisms: Request-Response and Peer Delay, both of which assume a symmetric network.

11.1.6 Request-Response Mechanism

In the Request-Response mechanism, the master and slave clocks calculate the average path delay between them based on the PTP protocol messages they send and receive. If there is a TC between the master and slave clocks, the TC does not calculate the average path delay; it only forwards the received PTP protocol message and passes the Sync message's residence time on the TC to the slave clock.

The Request-Response mechanism figure is further divided into two modes: two-step mode and one-step mode, depending on whether the Follow_Up message needs to be sent:

- In two-step mode, as shown in Request-Response mechanism figure , the Sync message's sending timestamp t1 is carried by the Follow_Up message.
- In one-step mode, the Sync message's sending timestamp t1 is carried by the Sync message itself, and no Follow_Up message is sent.

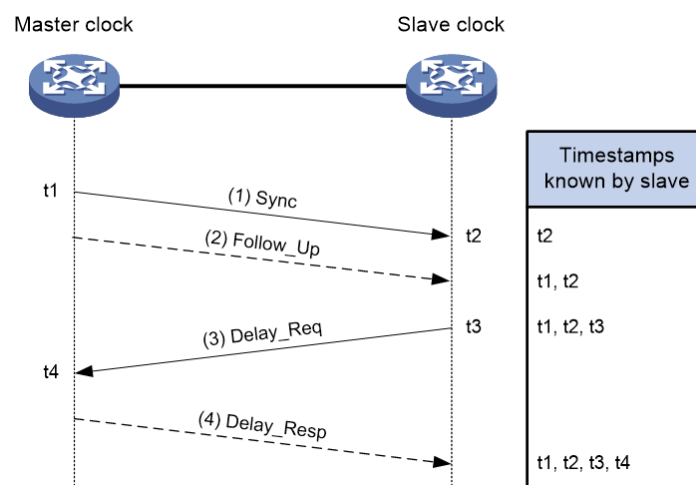
Request-Response mechanism figure explains the implementation process of the Request-Response mechanism in two-step mode:

1. The master clock sends a Sync message to the slave clock and records the sending time t1. The slave clock records the receiving time t2.
2. After sending the Sync message, the master clock immediately sends a Follow_Up message carrying t1.
3. The slave clock sends a Delay_Req message to the master clock to initiate the calculation of the reverse transmission delay and records the sending time t3. The master clock records the receiving time t4 after receiving this message.
4. After receiving the Delay_Req message, the master clock replies with a Delay_Resp message carrying t4.

At this point, the slave clock has the timestamps t1 to t4, and the following can be calculated:

- The round-trip delay between the master and slave clocks = $(t2 - t1) + (t4 - t3)$
- The one-way delay between the master and slave clocks = $[(t2 - t1) + (t4 - t3)] / 2$
- The clock offset of the slave clock relative to the master clock = $(t2 - t1) - [(t2 - t1) + (t4 - t3)] / 2 = [(t2 - t1) - (t4 - t3)] / 2$

Request-Response mechanism (two-step mode)



11.2 Principles of GPON Transmission Time

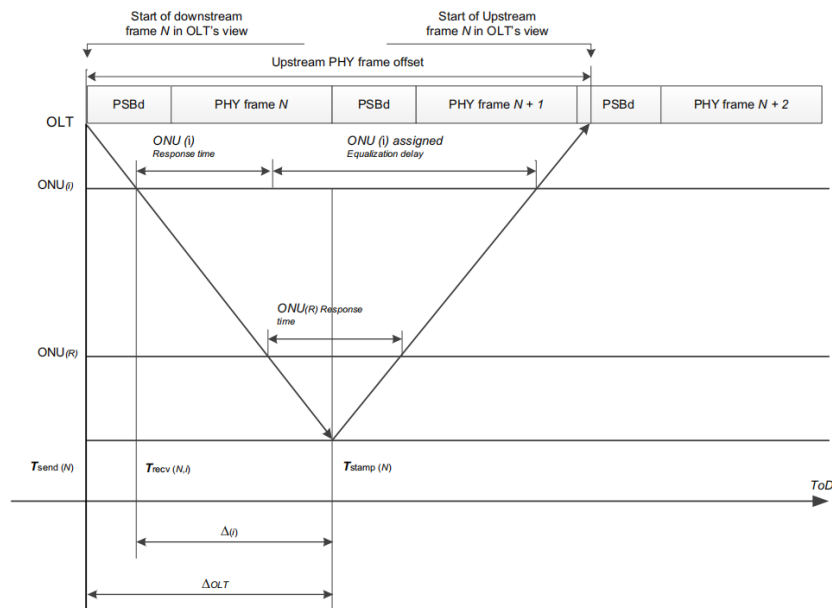
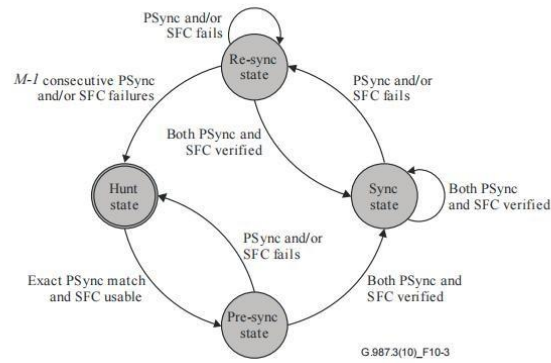
Time of day distribution over GPON/XGPON1, ITU-T G.984.3 amendment 2 (11/2009)/Section 10.4.6

(01/2014) and ITU-T G.987.3 Section 13.2 (01/2014) defines a method for the distribution ToD over the ODN portion of a GPON/XGPON1/XGS-PON network. The method defined is based on two factors: first, the GPON/XGPON1/XGS-PON network is frequency-synchronized with the OLT clock; and second, the propagation delays between the OLT and the ONU, in downstream and from ONU to the OLT in upstream, are continuously measured and controlled by the OLT. The principle of operation assumes that the OLT has an accurate real-time clock (RTC), obtained through means beyond the scope of these specifications. The OLT informs the ONU of the time of day when a certain downstream GTC/XGTC frame will arrive at a hypothetical ONU that has zero equalization delay and zero ONU response time. The certain downstream frame is identified by N, the value of its super-frame counter (SFC), which is an existing feature of the protocol.

The information transfer is accomplished using the OMCI channel and does not need to be in real time. When the selected frame arrives at the ONU, the ONU uses this ToD information, its equalization delay, and its response time to compute its local clock with very high accuracy.

According to the algorithm and method described in ITU-T G.984.3/G.987.3, the quantities required for ToD calculation and generation at the OLT, are $T_{send}(N)$, which is the time of transmission of frame number N at the OLT, and T_{eqd} , the zero distance equalization delay (also called PON Distance).

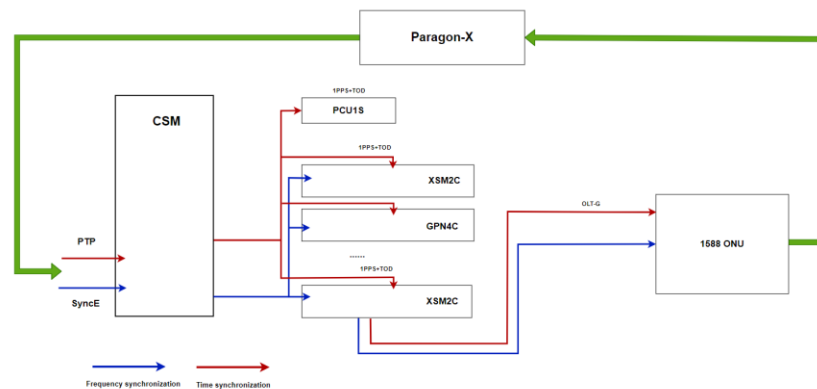
The quantities required for the calculation of the ToD in ONU(i) (ONU number i) are the sum of the equalization delay $EqD(i)$ that is given to ONU(i) during ranging and the response time ($RespTime(i)$), which is the response time of ONU(i). This document suggests a procedure for the generation of the quantity $T_{send}(N)$ in the OLT. It is assumed that the quantity T_{eqd} is known by configuration, and does not change frequently throughout the link activation period. ONU frequency synchronization with the OLT during registration.



11.3 PTP Configuration Instance

11.3.1 Application Description

The AX3500 series use SyncE + PTP to transmit accurate time, with SyncE providing frequency synchronization and PTP providing time synchronization. Paragon-X is an instrument for testing the 1588 function, and it is equipped with a high-precision rubidium clock to maintain stable frequency. The OLT can be understood to have two main control sections (CSM) for PTP and SyncE functions. The service cards use the downlink broadcast signal during the registration phase to keep the ONU's frequency consistent, and through the OMCI message, the OLT-G ToD field transmits precise time to the ONU.



11.3.2 Configuration Requirements

- The Grand Master Clock supports the 1588 function with One-step/Two-step Layer 2 multicast message format.
- The ONU itself has a high-precision clock chip and must support the 1588 function.

11.3.3 Operating Steps

- Configure Uplink Port SyncE
- Configure Port PTP Parameters
- Enable ToD to Slot
- View PTP Configuration
- Configure 1588 Function for ONU
- Check 1588 Test Results

11.3.3.1 Configure Uplink Port SyncE

Configure the uplink port XGE1 SyncE function, see Chapter 9 for details.

11.3.3.2 Configure Port PTP Parameters

- Set the uplink port XGE1 PTP domain to 24.
AX3517#configure ptp AX3517(PTP)#domain 24
- Enable PTP function on the uplink port XGE1.
AX3517(PTP)# ethport-ptp xge 1 enable on
- Set the local priority of the uplink port XGE1 PTP to 128.
AX3517(PTP)# ethport-ptp xge 1 localpriority 128
- Set the uplink port XGE1 PTP message to untagged.
AX3517(PTP)# ethport-ptp xge 1 vlanid 0
- Configure the uplink port XGE1 PTP Announce message to 8 per second with a timeout of 3 seconds.
AX3517(PTP)# ethport-ptp xge 1 anncintv -3 annctmo 3
- Set the uplink port XGE1 PTP Sync message to 8 per second (no Sync messages are sent when the port role is Slave).
AX3517(PTP)# ethport-ptp xge 1 syncintv -3
- Set the local priority of the uplink port XGE1 PTP to 128. Set the uplink port XGE1 PTP Del-request message to 8 per second (no Del-request messages are sent when the port role is Master).
AX3517(PTP)# ethport-ptp xge 1 delreqintv -3

11.3.3.3 Enable ToD to Slot

- Enable the main control to send ToD to Slot 3 service card.
AX3517(PTP)#slot-tod 3 enable

11.3.3.4 View PTP Configuration

AX3517(PTP)#show config

Config priority1 128

Config priority2 128

Config clockaccuracy 187

Config clockclass 254

Config domain 24

Config bmcenable :enable

Config slaveonly :disable

Config filterenable :enable

Config todrxtype :time

Config todtxtype :time

Config bmcprofile: default

Config stimetraceable: -1

Config variance 2400

Config sclockclass :-1

Config sgmprio1 :-1

Config sgmprio2 :-1

Config scorrection :-1

Config sclockvariance :-1

Config syncing :Synced

tod slot 3 :enable

tod slot 5 :disbale

tod slot 6 :disbale

AX3517(PTP)#

AX3517(PTP)#show config ethport-ntp

Index	Enable E/P	Role	Step	PdelReqIntv	AnncIntv	SyncIntv	DelreqIntv	
AnncTmo	Vid	TPID	TTL	IoPri	Cos	DSCP	Dstmactip	Srcip
Transport								
xge 1	Yes	E2E	auto	One	-4	-3	-3	-3
3	0	0x8100	255	128	7	0x38	01:00:5e:00:01:81	0.0.0.0
0.0.0.0	Ethernet							

```

xge 2   No      E2E  auto  One  -4      1      0      0
4       1      0x8100 255  0      7      0x38 01:00:5e:00:01:81  0.0.0.0
0.0.0.0      Ethernet

xge 3   No      E2E  auto  One  -4      1      0      0
4       1      0x8100 255  0      7      0x38 01:00:5e:00:01:81  0.0.0.0
0.0.0.0      Ethernet

xge 4   No      E2E  auto  One  -4      1      0      0
4       1      0x8100 255  0      7      0x38 01:00:5e:00:01:81  0.0.0.0
0.0.0.0      Ethernet

xge 5   No      E2E  auto  One  -4      1      0      0
4       1      0x8100 255  0      7      0x38 01:00:5e:00:01:81  0.0.0.0
0.0.0.0      Ethernet

xge 6   No      E2E  auto  One  -4      1      0      0
4       1      0x8100 255  0      7      0x38 01:00:5e:00:01:81  0.0.0.0
0.0.0.0      Ethernet

xge 7   No      E2E  auto  One  -4      1      0      0
4       1      0x8100 255  0      7      0x38 01:00:5e:00:01:81  0.0.0.0
0.0.0.0      Ethernet

xge 8   No      E2E  auto  One  -4      1      0      0
4       1      0x8100 255  0      7      0x38 01:00:5e:00:01:81  0.0.0.0
0.0.0.0      Ethernet
    
```

AX3517(PTP)#

11.3.3.5 View PTP Configuration

- Create an ONU service template.

```

AX3517(Slot-3)#gpon profile flow id 3 1 name 1 uni-type ethernet- uni uni-
bitmap 0x1 upmap-type vlanId 101 101 pri-bitmap 0xff vport 1
AX3517(Slot-3)#
    
```

- Register the ONU and configure the basic services for the ONU.

```

AX3517#brief-show slot 3 ont-unbound
    
```

Index: 1.

Onu Type: XGSPON.

Onuld: slot-[3] device-[1] link-[1] onu-[0].

Serial Number: APHN30303130 Vendor-Id[41 50 48 4E] Specific[30 30
31 30].

RegistrationId:

00
0000

00

Reason: SERIAL_NUM_NOT_KNOWN

AX3517#slot 3

AX3517(Slot-3)#interface gpon-olt 1/1 AX3517(Slot-3/if-gpon-olt-1/1)#ont 1

AX3517(Slot-3/if-gpon-olt-1/1/1)#sn APHN30303130 type xgspn

AX3517(Slot-3/if-gpon-olt-1/1/1)#virtual-port 1 port unlock

AX3517(Slot-3/if-gpon-olt-1/1/1)#service flow-profile 3 tcont- bind-profile 1 svc-type 1_p

- Configure the ONU 1588-related parameters, such as setting the domain to 24, mode to one-step, message format to multicast, and setting message intervals, etc.

AX3517(Slot-3/if-gpon-olt-1/1/1)#

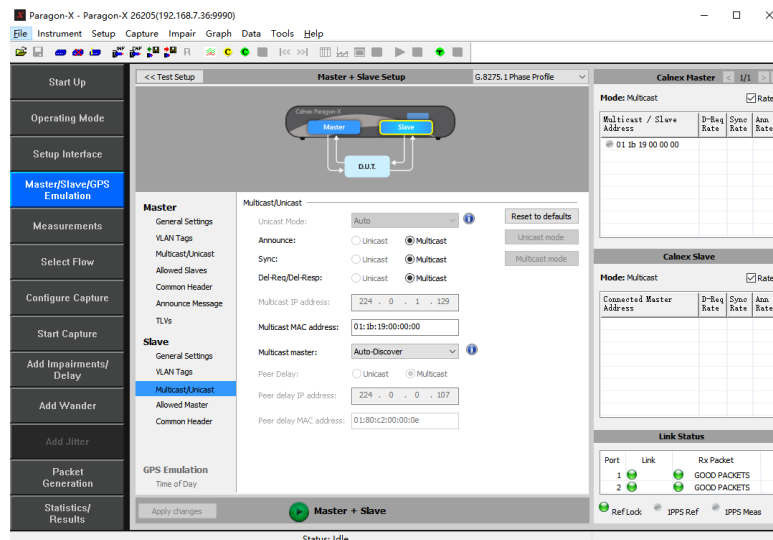
AX3517(Slot-3/if-gpon-olt-1/1/1)# time-status-message domainNo 24 priority1
128 accuracy 0x20

AX3517(Slot-3/if-gpon-olt-1/1/1)# ptp-config admin-state lock

comm-model multicast clock-step one_step log-ann-intvl 6 log-syn-intvl 5

11.3.3.6 Check 1588 Test Results

- Status when the instrument has 1588 disabled.



AX3517(PTP)#show status

```

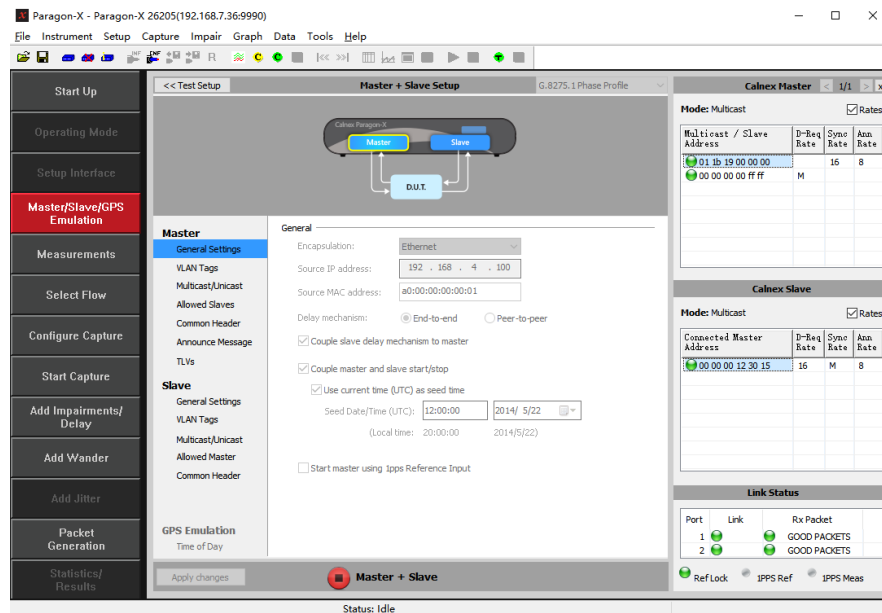
clock id                                     :005699.FFFE.CC00AC
parent clock id                             :005699.FFFE.CC00AC
gm clock id                                 :005699.FFFE.CC00AC
mean path delay                             0
offset from master                          0
time offset                                 0
gm prio1                                    128
gm prio2                                    128
gm clockclass                               254
gm clockaccuracy                            187
time source                                 :internal_oscillator
steps removed                               0
clock type                                  :oc
parent Stats                                :disable
gm variance                                 2400
variance from parent                        65535
phase change rate                           2147483647
current utc offset                          37
    
```

AX3517(PTP)#show status ethport-ptp

Index	State	Offset
xge 1	master	-1879048193
xge 2	disable	-1879048193
xge 3	disable	-1879048193
xge 4	master	-1879048193
xge 5	disable	-1879048193
xge 6	disable	-1879048193
xge 7	disable	-1879048193
xge 8	disable	-1879048193

AX3517(PTP)#

- Instrument with 1588 test enabled.

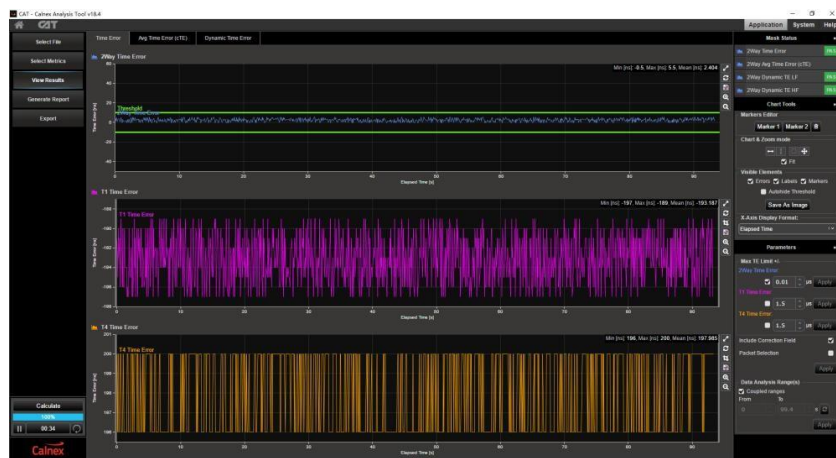
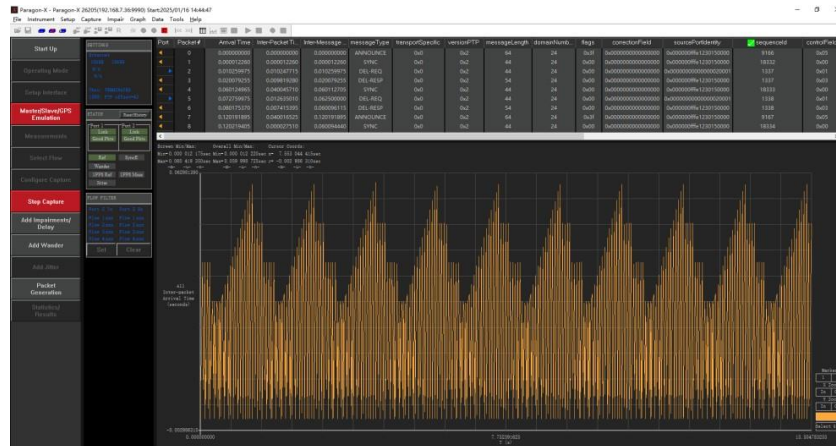


```
AX3517(PTP)# show status
clock id                :005699.FFFE.CC00AC
parent clock id         :000000.0000.000001
gm clock id             :000000.0000.000001
mean path delay         :198574080
offset from master      :-196608
time offset             :-196608
gm prio1                :128
gm prio2                :128
gm clockclass           :6
gm clockaccuracy        :33
time source             :internal_oscillator
steps removed           :1
clock type              :oc
parent Stats            :disable
gm variance             :-1
variance from parent    65535
phase change rate       2147483647
current utc offset      37
```

```
AX3517(PTP)#show status ethport-ptp
```

Index	State	Offset
xge 1	slave	3
xge 2	disable	-1879048193
xge 3	disable	-1879048193
xge 4	disable	-1879048193
xge 5	disable	-1879048193
xge 6	disable	-1879048193
xge 7	disable	-1879048193
xge 8	disable	-1879048193

- Result.



- The main focus is on the 2Way Time Error, which is generally required to be within ± 50 ns.



- Subsequently, stability testing is performed as needed. The following figure shows the test results after approximately 3 hours (for illustration purposes only).



12 External Alarm Input/Output

12.1 Introduction

Network devices are generally installed on racks in user data centers, where audible and visual alarm devices are typically installed.

When a network device generates an alarm of a certain level, the device needs to output the alarm status of the network element to the audible and visual alarm devices on the rack, usually a buzzer or large alarm light, to alert the data center administrators to handle anomalies.

Typically, a rack doesn't only have one network device, but the input for the audible and visual alarm devices may be limited to one channel. Therefore, the network device must also output alarms from other network devices as alarm inputs, manage them as its own alarm inputs, and then output them together to the audible and visual alarm devices, so that alarms from all network devices in the same rack can be handled collectively. When an alarm input is enabled and detects a valid input, an external input alarm must be reported.

12.2 Product Specifications

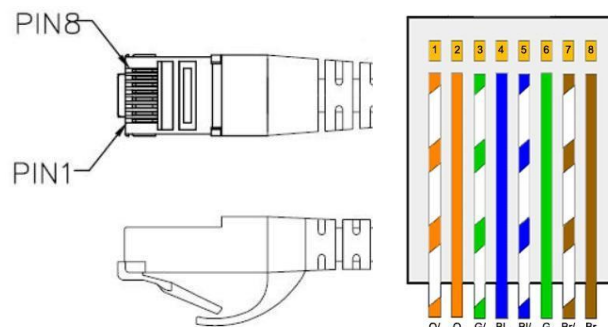
The AX3508/AX3515/S17 chassis is equipped with a PCU1S board, which supports 7 alarm inputs and 1 alarm output. The ALM1 interface supports 4 alarm inputs, while the ALM2 interface supports 3 alarm inputs and 1 alarm output.

The alarm input/output of the AX3502 is placed on the CSM2S/CSM2SL control board. The CSM2S/CSM2SL supports 6 alarm inputs and 2 alarm outputs. Each board's ALM interface supports 3 alarm inputs and 1 alarm output.

12.3 Operating Steps

Alarm Interface Cable: Prepare a network cable with a crystal head on one side and connect it to the device's ALM port. The other side should be connected as shown in the diagram, with pairs connected as follows:

- Pin 1 - Pin 2: Orange - Orange/White (Input 1)
- Pin 3 - Pin 4: Blue - Green/White (Input 2)
- Pin 5 - Pin 6: Green - Blue/White (Input 3)
- Pin 7 - Pin 8: Brown - Brown/White (Output)



12.3.1 Configure Alarm Input

Alarm Input Command

AX3517#external-alarm-input 1 enable valid-value on alarm-level critical

12.3.2 Configure Alarm Output

Alarm Output Command

AX3517#external-alarm-output 1 enable valid-value on manual-mode un-manual alarm-level critical

The input and output ports will be monitored every minute, and alarms will be reported or cleared accordingly.

12.3.3 Querying Alarms

- Query alarm information

AX3517#brief-show alarm

Num	Seq	Alarm Name	Severity	Occurred	Time
Entity Type	Entity Ins				
-----+-----+-----+-----+-----					
---+-----+-----+-----					
1	15	External Alarm	critical	2024/08/17,	
13:12:41	External	ExternalAlarm-1			

- Query external alarm input and output

AX3517#brief-show external-alarm

AX3517#alarm

AX3517(ALARM)#show external-alarm

PCU1S SW Version: A7

Input Id	State	Alarm Level	Valid
Value	Current Value		
1	disable	major	off
on			
2	disable	major	off
on			
3	disable	major	off
on			
4	disable	major	off
on			

5 on	disable	major	off
6 on	disable	major	off
7 on	disable	major	off

Output Id	State	Alarm Level	Manual
Mode	Valid Value	Current Value	

1 un-manual	disable off	critical off	

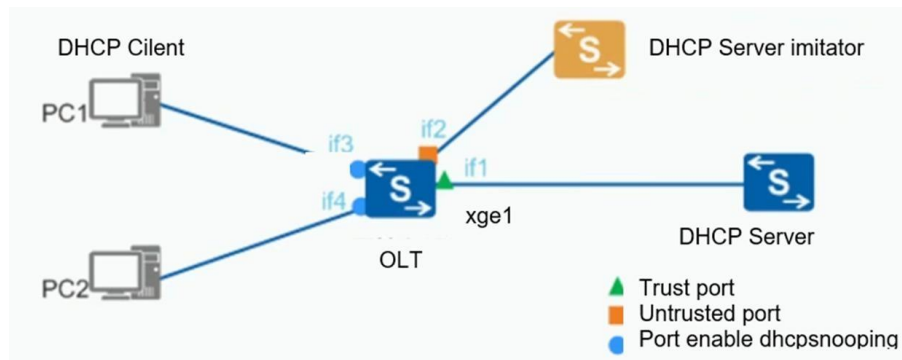
13 Security

This section describes how to configure system security options to ensure that data in the OLT is protected from external attacks.

13.1 DHCP Snooping

DHCP Snooping is a DHCP security feature to shield unauthorized DHCP servers from the network. After DHCP Snooping is enabled, clients on the network can obtain IP addresses only from the DHCP server specified by the administrator. DHCP packets lack the authentication mechanism. If an invalid DHCP server exists on the network, the administrator cannot ensure that the client obtains a valid IP address from the DHCP server specified by the administrator. As a result, the client may obtain incorrect configuration information such as an IP address from the invalid DHCP server. After DHCP Snooping is enabled, the ports on the device must be set to the Trust and Untrust state. The switch forwards DHCP OFFER/ACK/NAK messages only from the trusted ports. The DHCP OFFER/ACK/NAK packets from untrusted ports are discarded to block unauthorized DHCP servers.

13.1.1 Topology Instance



13.1.2 Topology Instance

1. Configure DHCP snooping

```
AX3517(CONFIG/Security)#dhcp snooping<enable | disable>
```

2. After xge 1 is configured as the dhcp trusted port, the dhcp server OFFER/ACK/NAK packets received by xge 1 are forwarded

```
AX3517(CONFIG/Security)#trust-port interface xge 1 dhcp enable
```


13.2 PPPOE Snooping

Mask the invalid PPPOE server on the access network. After PPPOE Snooping is enabled, network clients can obtain IP addresses only from the PPPOE server specified by the administrator

1. Configure PPPOE snooping

```
AX3517(CONFIG/Security)#pppoe-snooping <enable|disable>
```

2. Configure the upper and internal interfaces as trusted ports

```
AX3517(CONFIG/Security)#trust-port interface xge 1 pppoe enable
```

```
AX3517(CONFIG/Security)#trust-port interface is 1/1 pppoe enable
```

13.3 Anti-MAC-Spoofing

Method of filtering based on MAC address. You can set rules to allow or deny network access based on the MAC address of a network device

```
AX3517(CONFIG/Security)#anti-mac-spoofing <enable|disable>
```

13.4 ARP Snooping

The following is the arp snooping function

- Check whether the source MAC of the ARP Reply packet header is the same as that of the Sender in the Reply data area. If no, the packet is discarded.
- Capture ARP Reply packets, generate an ARP binding table, and periodically check aging.

After receiving downstream ARP request messages, if DHCP Snooping is enabled and DHCP is associated with ARP, the DHCP table is directly sent to the ONU of the switch. Otherwise, the ARP table is bound to the ONU of the switch.

```
AX3517(CONFIG/Security/ARP)#snooping <enable|disable>
```

13.5 IP-MAC-Bind

After this function is enabled, IP address spoofing can be prevented

1. Configure ARP snooping

```
AX3517(CONFIG/Security)#ip-mac-bind 1.2.3.4 11:22:33:44:55:66
```

2. View the ARP binding table

```
AX3517(CONFIG/Security/ARP)#show bind-table
```

13.6 MAC Force Forwarding

In many network scenarios, gateways are needed to monitor data traffic, and users cannot communicate with each other directly, that is, two-layer isolation and three-layer interoperability between different users are needed. Deploying MFF function can perform two-layer isolation and three-layer intercommunication for users in the same network segment. Through layer 2 isolation, traffic can be directed to the gateway to realize traffic monitoring, accounting and other applications, as well as to ensure the security of the network environment.



Note: ARP snooping must be enabled in advance.

1. Configure mac-force-forwarding

```
AX3517(CONFIG/Security/ARP)#mac-force-forwarding <enable|disable>
```

2. Configure the default gateway

```
AX3517(CONFIG/Security/ARP)#mac-force-forwarding default-gateway 192.168.10.1
```

3. View the default gateway configuration

```
AX3517(CONFIG/Security/ARP)#mac-force-forwarding show default-gateway.
```

14 Performance Statistics

14.1 View Performance Statistics

View XGE/GE/LAG port statistics:

```
AX3517# configure AX3517(CONFIG)# l2
```

```
AX3517(CONFIG/L2)# bridge
```

```
AX3517(CONFIG/L2/BRIDGE)# show statistics <xge|is|trunk> <intf-id>
```

View PON port statistics:

```
AX3517# brief-show slot 13 interface gpon-olt <intf-id> counters
```

View GEM Port Statistics:

```
AX3517# brief-show interface gpon-olt <intf-id> counters gempport  
<port-id>
```

Viewing Multicast GEM Port Statistics:

```
AX3517#brief-show interface gpon-olt <intf-id> counters multicast  
<ONU-id>
```

View ONU statistics on PON:

```
AX3517# brief-show interface gpon-olt <intf-id> counters ont <id>
```

14.2 Clear Performance Statistics

Clear master card statistics:

```
AX3517(CONFIG/L2/BRIDGE)# clear counter-csm counter <xge|is|trunk>  
<intf-id>
```

Clear statistics for line card nni/gemport/ont:

```
AX3517#clear counter-lc <slot id> gpon-olt <1/port id>  
<nni|ont|ont-counts>
```

15 System Administration

This chapter describes the system management functions.

The following sections describe in detail how to perform system administration tasks:

- Equipment document management
- Save configuration
- Reboot system_Equipment document management
- Active-standby switchover
- System upgrade

15.1 Equipment Document Management

AX3517/AX3515/AX3508/AX3502Device files are stored in the network directory/tftpboot/and the basic file operation commands are as follows:

```
AX3517# show file AX3517# no file
```

File name	Explain	Directory
csm1g.gz	OLT image file	/tftpboot/
sys_version_file	system version file	/tftpboot/
csm1g-kernel.bin	CSM1G kernel file	/tftpboot/
csm1g-rootfs.bin	CSM1G root file system	/tftpboot/
csm1g-p1021.dtb	CSM1G CPU Support File	/tftpboot/
csm1g-uboot.bin	CSM1G startup file	/tftpboot/
csm1g-userfs.jffAX3502	CSM1G User File System	/tftpboot/
gpn2.img	GPN2A , GPN2C image files	/tftpboot/
xgn1a.img	XGN1A image file	/tftpboot/
xgs1d.img	XGN1D image file	/tftpboot/
xsm1a.img	XSM1A image file	/tftpboot/
sysconfig.gz	system configuration file	/tftpboot/
bcm68620_appl.bin	PON Application Document	/tftpboot/
bcm68620_boot.bin	PON startup file	/tftpboot/

15.2 Save Configuration

Save the current configuration of the system to memory, so that these configurations are still valid after the system is restarted. Otherwise, the system restarts and all user configurations will be invalid.

```
AX3517# save config
```

```
Are you sure you want to save the configuration ? (yes or no) y
```

```
save success!
```

15.3 Reboot System

Restart the line card using the following command :

```
AX3517# reset slot 1-2 <soft|hard>
```



Note: In the above command, "1-2" means to restart the board in slot 2.

Reboot the system with the following command:

```
AX3517# resetnode
```

15.4 Active-Standby Switchover

AX3517/AX3515/AX3508/AX3502 supports the backup of the main control card. If the main card fails, it will automatically switch to the standby board. It also supports manual switching. The switching can be configured first:

- Automatically synchronize the master and backup files of the master control card:

```
AX3517# sync-option enable
```

- Manual sync:

```
AX3517# manual-sync CSM
```

- To switch the active and standby main control cards:

```
AX3517# switchover CSM
```

15.5 System Upgrade

AX3517/AX3515/AX3508/AX3502 upgrade is divided into CSM upgrade and line card upgrade.

15.5.1 CSM Upgrade

- Save and backup configuration file.

```
AX3517# save config
```

```
Are you sure you want to save the configuration ? (yes or no) y
```

```
save success!
```

```
AX3517# upload ip 192.168.10.10 src /tftpboot/sysconfig.gz dst sysconfigbak.gz
```

- Active and standby synchronization.

```
AX3517# manual-sync CSM
```

- Transfer the upgrade file to the tftpboot directory through WinSCP, and then use the following command to confirm the image file, and wait for the confirmation to succeed.

```
AX3517# commit-image both
```

```
AX3517# show image-commit-status
```

```
Slot A      Active      successful
```

```
Slot B      Standby     successful
```

- Reboot the system.

```
AX3517# resetnode
```

15.5.2 Line Card Upgrade

- Backup configuration files.

```
AX3517# save config
```

```
Are you sure you want to save the configuration ? (yes or no) y
```

```
save success!
```

```
AX3517# upload ip 192.168.10.10 src /tftpboot/sysconfig.gz dst sysconfigbak.gz
```

- Upgrade the line card.

Transfer the upgrade file to the tftpboot directory through WinSCP, and then use the following command to upgrade.

```
AX3517# upgrade-lc slot 1 src /tftpboot/gpn2.img
```

- Restart the line card.

```
AX3517# reset slot 1-1
```



Ascent Communication Technology Ltd

AUSTRALIA

140 William Street, Melbourne
Victoria 3000, AUSTRALIA
Phone: +61-3-8691 2902

Hong Kong SAR

Unit 9, 12th Floor, Wing Tuck Commercial Centre
177 Wing Lok Street, Sheung Wan, Hong Kong SAR
Phone: +852-2851 4722

CHINA

Unit 1933, 600 Luban Road
200023, Shanghai CHINA
Phone: +86-21-60232616

USA

2710 Thomes Ave
Cheyenne, WY 82001, USA
Phone: + 1 203 350 9822

EUROPE

Pfarrer-Bensheimer-Strasse 7a
55129 Mainz, GERMANY
Phone: +49 (0) 6136 926 3246

VIETNAM

11th Floor, Hoa Binh Office Tower
106 Hoang Quoc Viet Street, Nghia Do Ward
Cau Giay District, Hanoi 10649, VIETNAM
Phone: +84-24-37955917

WEB: www.ascentcomtec.com

EMAIL: sales@ascentcomtec.com

Specifications and product availability are subject to change without notice.
Copyright © 2025 Ascent Communication Technology Limited. All rights reserved.
Ver. ACT_AX3500_XGSPON_OLT_CLI_Operation_QRG_V1b_Jun_2024